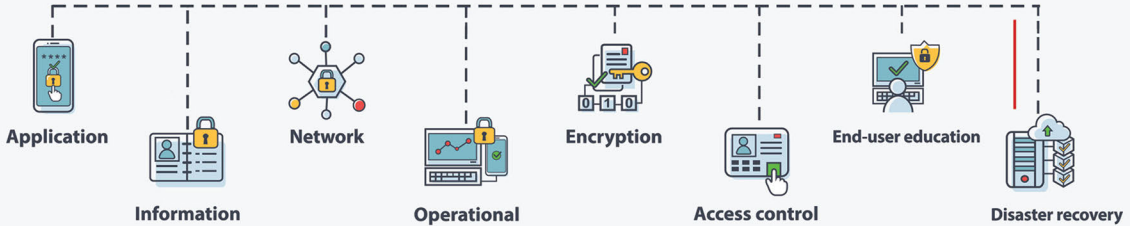




CYBER SECURITY



CYBER SECURITY FOR NEXT-GENERATION COMPUTING TECHNOLOGIES

Edited by

Inam Ullah Khan, Mariya Ouaisa,
Mariyam Ouaisa, Zakaria Abou El Houda,
and Muhammad Fazal Ijaz



CRC Press
Taylor & Francis Group

Cyber Security for Next-Generation Computing Technologies

This book sheds light on the cyber security challenges associated with next-generation computing technologies, emphasizing the serious threats posed to individuals, businesses, and nations. With everything becoming increasingly interconnected via the Internet, data security becomes paramount. As technology advances, people need to secure their data communication processes. Personal data security, including data integrity and confidentiality, is particularly vulnerable. Therefore, the concept of cyber security forensics emerges to ensure data security for everyone, addressing issues such as data control, hijacking, and threats to personal devices such as mobile phones, laptops, and other smart technologies. This book covers key topics related to cyber security in next-generation computing technologies, ultimately enhancing the quality of life for citizens, facilitating interaction with smart governments, and promoting secure communication processes.

KEY FEATURES

- Highlights innovative principles and practices using next generation computing technologies based cybersecurity.
- Presents an introduction to recent trends regarding the convergence of AI/ML in cybersecurity
- Offers an overview of theoretical, practical, simulation concepts of cybersecurity



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Cyber Security for Next-Generation Computing Technologies

Edited by Inam Ullah Khan, Mariya Ouaisa,
Mariyam Ouaisa, Zakaria Abou El Houda,
and Muhammad Fazal Ijaz



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Shutterstock

First edition published 2024

by CRC Press

2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press

4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© 2024 selection and editorial matter, Inam Ullah Khan, Mariya Ouaisa, Mariyam Ouaisa, Zakaria Abou El Houda and Muhammad Fazal Ijaz; individual chapters, the contributors

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-1-032-51899-2 (hbk)

ISBN: 978-1-032-51900-5 (pbk)

ISBN: 978-1-003-40436-1 (ebk)

DOI: 10.1201/9781003404361

Typeset in Times

by Apex CoVantage, LLC

Contents

Preface.....	vii
About the Editors.....	ix
List of Contributors.....	xiii
Chapter 1 Cyber Security: Future Trends and Solutions	1
<i>Syed Immamul Ansarullah, Mudasir Manzoor Kirmani, Ziema Mushtaq, and Gowhar Mohi ud din Dar</i>	
Chapter 2 Security and Intelligent Management: Survey.....	16
<i>Zaigham Abbas, Abdul Qahar Shahzad, Muhammad Yaseen Ayub, and Muhammad Allah Rakha</i>	
Chapter 3 Comparative Analysis of Machine and Deep Learning for Cyber Security	39
<i>Hafsa Maryam, Syeda Zillay Nain Zukhraf, and Rehmat Ullah</i>	
Chapter 4 AI-Based Secure Wireless Communication Technologies and Cyber Threats for IoT Networks	70
<i>Usman Haider, Bakhtawar Nawaal, Inam Ullah Khan, and Salma El Hajjami</i>	
Chapter 5 Cyber Threat Actors Review: Examining the Tactics and Motivations of Adversaries in the Cyber Landscape	84
<i>Zakaria Abou El Houda</i>	
Chapter 6 Layer-Based Security Threats in IoT Networks	102
<i>Muna Muhammad, Ahthasham Sajid, and Hira Arshad</i>	
Chapter 7 Intrusion Detection System Using AI and Machine Learning Algorithm	120
<i>Muhammad Tehmasib Ali Tashfeen</i>	
Chapter 8 Signature-Based Intrusion Detection System for IoT.....	141
<i>Bakhtawar Nawaal, Usman Haider, Inam Ullah Khan, and Muhammad Fayaz</i>	

Chapter 9	Hybrid Model for IoT-Enabled Intelligent Towns Using the MQTT-IoT-IDS2020 Dataset.....	159
	<i>Zupash, Muhammad Allah Rakha, Inam Ullah Khan, Mariya Ouaisa, Mariyam Ouaisa, and Muhammad Yaseen Ayub</i>	
Chapter 10	Cyber Security for Edge/Fog Computing Applications	177
	<i>Hanane Lamaazi</i>	
Chapter 11	Cyber Attacks Against Intelligent Transportation Systems	190
	<i>Muhammad Usama, Ubaid Ullah, and Ahthasham Sajid</i>	
Chapter 12	Intelligent Transportation Systems for IoT-Based UAV Networks.....	231
	<i>Mamoonah Jamil, Usman Haider, Inam Ullah Khan, and Tarandeep Kaur Bhatia</i>	
Chapter 13	Cyber Attack Detection Analysis Using Machine Learning for IoT-Based UAV Network	253
	<i>Usman Haider, Hina Shoukat, Muhammad Yaseen Ayub, Muhammad Tehmasib Ali Tashfeen, Tarandeep Kaur Bhatia, and Inam Ullah Khan</i>	
Chapter 14	Blockchain Solutions for Cyber Criminals	265
	<i>Vijendra Kumar Maurya, Denis Jangeed, Latif Khan, and Bhupendra Kumar Soni</i>	
Chapter 15	Blockchain Security Measures to Combat Cyber Crime	275
	<i>Rahmeh Ibrahim and Qasem Abu Al-Haija</i>	
Chapter 16	AI Classification Algorithms for Human Activities Recognition System With a Cyber Security Perspective	294
	<i>Fahad Naveed, Shahbaz Ali Imran, Aftab Alam Janisar, Aliyu Yusuf, Salman Khan, and Inam Ullah Khan</i>	

Preface

The field of cyber security has recently gained significant importance as the challenge of securing information transmission becomes crucial. The advent of smart IT infrastructure has revolutionized the global landscape, but it has also brought forth security concerns. Consequently, cyber crimes have witnessed a steady rise over time, involving activities such as identity theft, bullying, terrorism, and network disruptions. In this smart world, privacy and security have become indispensable for individuals. Fortunately, the next generation of computing technologies, including IoT/IoE, artificial intelligence, machine learning, deep learning, smart grid, ad hoc networks, SDN, network security, big data, image processing, and green communication, offers potential solutions.

The integration of these fields encompasses cyber attacks, forensic analysis, and privacy issues, necessitating exploration through optimization techniques and evolutionary computations. Next-generation computing finds diverse applications in areas like smart infrastructure, air quality monitoring, waste management, school management, healthcare, and telemedicine. These applications rely on security measures to facilitate optimal decision making in real time. Ad hoc networks play a crucial role in reducing end-to-end delays and connectivity problems, while wireless communication technology serves as the backbone of future networks. Governments, enterprises, and individuals must prioritize cyber security and utilize forensic techniques to protect data when sharing it with others, as privacy concerns arise due to potential security breaches during extensive data sharing. Analyzing complex information and real-time data is essential for ensuring the sustainability of future networks and related applications.

This book sheds light on the cyber security challenges associated with next-generation computing technologies, emphasizing the serious threats posed to individuals, businesses, and nations. With everything becoming increasingly interconnected via the Internet, data security becomes paramount. As technology advances, people need to secure their data communication processes. Personal data security, including data integrity and confidentiality, is particularly vulnerable. Therefore, the concept of cyber security forensics emerges to ensure data security for everyone, addressing issues such as data control, hijacking, and threats to personal devices such as mobile phones, laptops, and other smart technologies. This book covers key topics related to cyber security in next-generation computing technologies, ultimately enhancing the quality of life for citizens, facilitating interaction with smart governments, and promoting secure communication processes.

Chapter 1 provides an overview of cyber security, exploring its impact on businesses and analyzing recent trends and future solutions. Chapter 2 focuses on security and intelligent management to ensure system safety. Chapter 3 presents a comprehensive study of machine learning (ML) and deep learning (DL) techniques for detecting potential cyber attacks, while Chapter 4 surveys AI-based applications, intrusion detection systems (IDS), cyber attacks on IoT networks, and AI tools.

Chapter 5 aims to investigate the tactics and motivations of cyber threat actors in the current cyber security landscape, while Chapter 6 conducts a detailed review of security threats and attacks across different layers of IoT systems. Chapter 7 demonstrates how an intrusion detection system using AI and ML can function effectively out of the box, and Chapter 8 provides a detailed survey on signature-based IDS for IoT environments. In Chapter 9, a hybrid model is proposed for identifying attacks on IoT-enabled smart cities.

Chapter 10 offers an overview of cyber security in edge/fog computing applications, highlighting potential risks, common attack vectors, and best practices for security. Chapter 11 explores various cyber security attacks targeting intelligent transportation systems (ITS), including phishing attacks, malware, remote access, denial of service (DoS) attacks, physical attacks, insider threats, and social engineering. Chapter 12 presents a comprehensive survey of security attacks in UAV networks and other intelligent transportation systems, while Chapter 13 conducts a comparative study of machine learning techniques to investigate trust in IoT-based aerial ad hoc networks.

Chapter 14 delves into the applications of blockchain technology in cyber security and the security solutions it offers, while Chapter 15 expands on blockchain concepts, components, architecture, features, types, and limitations. Lastly, Chapter 16 focuses on human activity recognition problems from a cyber security perspective, proposing a novel method for accurate human activity recognition through different algorithms.

About the Editors

Dr. Inam Ullah Khan is a visiting researcher at King's College London, UK. Dr. Khan was a lecturer at different universities in Pakistan, including the Center for Emerging Sciences Engineering & Technology (CESET), Islamabad, Abdul Wali Khan University, Garden and Timergara Campus, and University of Swat. He did his PhD in Electronics Engineering from the Department of Electronic Engineering, Isra University, Islamabad Campus, School of Engineering & Applied Sciences (SEAS). He completed his MS degree in Electronic Engineering at the Department of Electronic Engineering, Isra University, Islamabad Campus, School of Engineering & Applied Sciences (SEAS). He obtained his undergraduate degree in Bachelor of Computer Science from Abdul Wali Khan University Mardan, Pakistan. In addition, his master's thesis was published as a book, *Route Optimization with Ant Colony Optimization (ACO)* (Lambert Academic Publishing, 2017), in Germany, which is available on Amazon. He is a research scholar and has published research papers at the international level. More interestingly, he recently introduced a novel on routing protocol E-ANTHOCNET in the area of flying ad hoc networks. His research interests include network system security, intrusion detection, intrusion prevention, cryptography, optimization techniques, WSN, IoT, UAVs, mobile ad hoc networks (MANETS), flying ad hoc networks, and machine learning. He has served at international conferences as a technical program committee member, which include the EAI International Conference on Future Intelligent Vehicular Technologies, Islamabad, Pakistan, and the 2nd International Conference on Future Networks and Distributed Systems, Amman, Jordan, June 26–27, 2018, and has been recently working on the same level at the International Workshop on Computational Intelligence and Cybersecurity in Emergent Networks (CICEN'21) that will be held in conjunction with the 12th International Conference on Ambient Systems, Networks and Technologies (EUSPN 2021), which was co-organized in November 1–4, 2021, in Leuven, Belgium. He has published more than 20 research papers (including book chapters, peer-reviewed journal articles, and peer-reviewed conference manuscripts) and three edited books.

Dr. Mariya Ouaisa is currently a Professor in Cybersecurity and Networks at Cadi Ayyad University and a practitioner with industry and academic experience. She obtained a PhD in 2019 in Computer Science and Networks, at the Laboratory of Modelisation of Mathematics and Computer Science from ENSAM-Moulay Ismail University, Meknes, Morocco. She is a Networks and Telecoms Engineer, having graduated in 2013 from the National School of Applied Sciences, Khouribga, Morocco. She is a co-founder and IT consultant at the IT Support and Consulting Center. She worked for the School of Technology of Meknes Morocco as Visiting Professor from 2013 to 2021. She is a member of the International Association of Engineers and International Association of Online Engineering, and since 2021, she is an ACM Professional Member. She is Expert Reviewer with the Academic Exchange Information Centre (AEIC) and Brand Ambassador with Bentham Science. She has served and continues to serve on technical program and organizer committees of

several conferences and events and has organized many symposiums/workshops/conferences as a general chair and as a reviewer of numerous international journals. Dr. Ouaisa has made contributions in the fields of information security and privacy, Internet of Things security, and wireless and constrained networks security. Her main research topics are IoT, M2M, D2D, WSN, cellular networks, and vehicular networks. She has published over 40 papers (book chapters, international journals, and conferences/workshops), ten edited books, and eight special issues as guest editor.

Dr. Mariyam Ouaisa is currently Assistant Professor of Networks and Systems at Chouaib Doukkali University. She received her PhD degree in 2019 from the National Graduate School of Arts and Crafts, Meknes, Morocco, and her Engineering Degree in 2013 from the National School of Applied Sciences, Khouribga, Morocco. She is a communication and networking researcher and practitioner with industry and academic experience. Dr. Ouaisa's research is multidisciplinary and focused on the Internet of Things, M2M, WSN, vehicular communications and cellular networks, security networks, congestion overload problems, and resource allocation management and access control. She is serving as a reviewer for international journals and conferences, including IEEE access, wireless communications, and mobile computing. Since 2020, she is a member of the International Association of Engineers IAENG and International Association of Online Engineering, and since 2021, she is an ACM Professional Member. She has published more than 30 research papers (this includes book chapters, peer-reviewed journal articles, and peer-reviewed conference manuscripts), ten edited books, and six special issue as guest editor. She has served on program committees and organizing committees of several conferences and events and has organized many symposiums/workshops/conferences as a general chair.

Dr. Zakaria Abou El Houda is a researcher at the Université de Montréal, Montréal, Canada. He received an MSc degree in Computer Networks from Paul Sabatier University, Toulouse, France, his PhD degree in Computer Science from the University of Montréal, Canada, and PhD degree in Computer Engineering from the University of Technology of Troyes, Troyes, France. He has made contributions in the fields of information security, intrusion detection/prevention system, and security in software-defined networks. His current research interests include ML/DL-based intrusion detection, federated learning, and blockchain. He has also served and continues to serve on technical program committees and as a reviewer of several international conferences and journals, including *IEEE ICC*, *IEEE Globecom*, and *IEEE Transactions*.

Dr. Muhammad Fazal Ijaz received his BEng degree in Industrial Engineering and Management from University of the Punjab, Lahore, Pakistan, in 2011, and his DrEng degree in Industrial and Systems Engineering from Dongguk University, Seoul, South Korea, in 2019. From 2019 to 2020, he worked as Assistant Professor in the Department of Industrial and Systems Engineering, Dongguk University, Seoul, South Korea. Currently, he is working as Assistant Professor in the Department of

Intelligent Mechatronics Engineering, Sejong University, Seoul, Korea. He has published numerous research articles in several international peer-reviewed journals, including *Scientific Reports*, *IEEE Transactions on Industrial Informatics*, *IEEE Access*, *Sensors*, *Journal of Food Engineering*, *Applied Sciences*, and *Sustainability*. His research interests include machine learning, blockchain, healthcare engineering, the Internet of Things, big data, and data mining.



Taylor & Francis

Taylor & Francis Group

<http://taylorandfrancis.com>

Contributors

Zaigham Abbas

International Islamic University
Islamabad, Pakistan

Qasem Abu Al-Haija

Princess Sumaya University for
Technology
Jordan

Syed Immamul Ansarullah

Government Degree College Sumbal
Srinagar, India

Hira Arshad Baluchistan

University of Information Technology
Engineering and Management Sciences
Quetta, Baluchistan, Pakistan

Muhammad Yaseen

Ayub COMSATS University
Attock Campus, Pakistan

Tarandeep Kaur Bhatia

University of Petroleum and Energy
Studies (UPES)
Bidholi, India

Gowhar Mohi ud din Dar

Lovely Professional University
Phagwara, India

Salma El Hajjami

Ibnou Zohr University Agadir
Morocco

Zakaria Abou El Houda

L@bISEN, ISEN Yncréa Ouest
Carquefou, France

Muhammad Fayaz

University of Central Asia Naryn
Kyrgyzstan

Usman Haider

National University of Computer and
Emerging Sciences
Islamabad, Pakistan

Rahmeh Ibrahim

Princess Sumaya University for
Technology
Jordan

Shahbaz Ali

Imran Birmingham City University
Birmingham, UK

Mamoona Jamil

Isra University Islamabad
Pakistan

Denis Jangeed

Geetanjali Institute of Technical Studies
Udaipur, India

Aftab Alam Janisar

Universiti Teknologi Petronas
Seri Iskandar, Perak, Malaysia

Inam Ullah Khan

Isra University Islamabad Campus
Pakistan

Latif Khan

Geetanjali Institute of Technical
Studies
Udaipur, India

Salman Khan

Abdul Wali Khan University Mardan
Pakistan

Mudasir Manzoor Kirmani

FoFy, SKAUST-Kashmir
India

Hanane Lamaazi

College of Information Technology
UAE University, Abu Dhabi,
United Arab Emirates

Hafsa Maryam

University of Cyprus
Nicosia, Cyprus

Vijendra Kumar Maurya

Geetanjali Institute of Technical Studies
Udaipur, India

Muna Muhammad

Baluchistan University of Information
Technology Engineering and
Management Sciences
Quetta, Baluchistan, Pakistan

Ziema Mushtaq

Cluster University Srinagar
India

Fahad Naveed

Federal Urdu University of Arts Science
& Technology
Islamabad, Pakistan

Bakhtawar Nawaal

University of Engineering and
Technology
Taxila, Pakistan

Mariya Ouaisa

Cadi Ayyad University
Marrakech, Morocco

Mariyam Ouaisa

Chouaib Doukkali University
El Jadida, Morocco

Muhammad Allah Rakha

FAST National University
Peshawar, Pakistan

Ahthasham Sajid

Baluchistan University of Information
Technology Engineering and
Management Sciences
Quetta, Baluchistan, Pakistan

Abdul Qahar Shahzad

Quaid-I-Azam University
Islamabad, Pakistan

Hina Shoukat

COMSATS University Islamabad
Attock, Pakistan

Bhupendra Kumar Soni

Geetanjali Institute of Technical
Studies
Udaipur, India

Muhammad Tehmasib Ali Tashfeen

Wichita State University
Wichita, Kansas, United States

Rehmat Ullah

Cardiff Metropolitan University
Cardiff, UK

Ubaid Ullah

University of Wah
Wah Cantt, Pakistan

Muhammad Usama

University of Wah
Wah Cantt, Pakistan

Aliyu Yusuf

Universiti Teknologi Petronas
Seri Iskandar, Perak, Malaysia

Syeda Zillay Nain Zukhraf

University of Cyprus,
Nicosia, Cyprus
Department of Electrical Engineering
National University of Computer and
Emerging Sciences
Peshawar, Pakistan

Zupash

COMSATS University Islamabad
Attock, Pakistan

1 Cyber Security

Future Trends and Solutions

Syed Immamul Ansarullah, Mudasir Manzoor Kirmani, Ziena Mushtaq, and Gowhar Mohi ud din Dar

1.1 INTRODUCTION

Before the beginning of 1970, viruses, Trojan horses, worms, spyware, and malware were not even part of the mainstream lexicon of information technology. Robert Thomas, a BBN Technologies researcher in Cambridge, Massachusetts, created the first computer “worm” and named that “Creaper” [1]. By jumping between systems, the Creaper disseminated infection; to combat this virus, Ray Tomlinson created the Reaper, the first antivirus application that would seek out and destroy Creaper [2]. In 1988, Robert Morris desired to determine the magnitude of the Internet and to accomplish this, he developed software that accessed UNIX terminals, traversed networks, and cloned itself. The Morris worm was so destructive that it rendered computers unusable by substantially reducing their speed [3]. From that moment on, viruses became more lethal, pervasive, and difficult to manage. With it came the advent of cyber security.

The collective set of technology, methods, and procedures that businesses utilize to safeguard their computing environments from harm and unauthorized data access caused by online criminals or nefarious insiders is known as cyber security [4]. Organizations typically have a structure and system in place for dealing with attempted or successful cyber attacks. An effective framework can aid in threat detection and identification, network and system protection, and recovery in the event that an attack is successful. Cybersecurity is included in all systems that are vulnerable to threats and attacks to stop things like identity theft, cyber stalking, data loss, loss of sensitive data, and extortion attempts [5]. Sensitive information about themselves as well as their clients is held by critical infrastructures, including hospitals, financial services firms, power plants, etc. To operate without interruption, cyber threat researchers find new vulnerabilities, improve open-source tools, and inform people about the significance of cyber security. Since the introduction of the first mainframes, the CIA (confidentiality, integrity, and availability) triangle has been the de facto industry standard for computer security [6]. Figure 1.1 shows the CIA triad in cybersecurity.

- **Confidentiality:** Maintaining confidentiality requires not divulging information to unauthorized parties. It involves making an effort to safeguard the privacy and anonymity of authorized parties engaged in data sharing

and storage. Decrypting data that has been inadequately encrypted, man-in-the-middle (MITM) attacks, and disclosing sensitive information frequently compromise secrecy. Data encryption, two-factor authentication, biometric verification, security tokens, and other standard procedures are utilized to protect confidentiality.

- **Integrity:** Integrity relates to preventing unauthorized parties from altering information. It is required that information and programs can only be modified in certain and authorized ways. Integrity risks include turning a computer into a “zombie computer” and infecting online pages with malware. Typically, the following methods are used to ensure data integrity: cryptographic checksums, uninterrupted power supplies, data backups, etc.
- **Availability:** Availability ensures that the information is accessible to authorized users when required. Data is only helpful if it is accessible to the right people at the right time. Information inaccessibility may result from security vulnerabilities such as DDoS attacks, hardware failure, poor software, or human error. Common practices for ensuring availability include backing up data to external drives, installing firewalls, having a backup power supply, and replicating data.

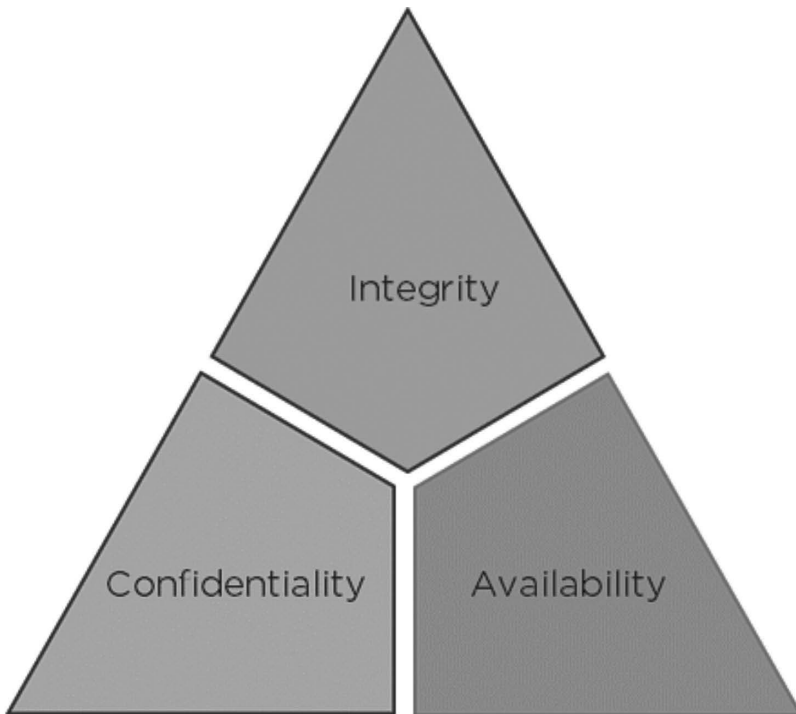


FIGURE 1.1 CIA (confidentiality, integrity, and availability) triad in cyber security.

1.2 TYPES OF CYBER SECURITY

Cyber security can broadly be divided into seven pillars [7–9]:

1. **Network Security:** A planned set of guidelines and configurations is used to secure networks and data by ensuring their confidentiality, integrity, and accessibility. By safeguarding the infrastructure, network security aims to defend internal networks from intruders. The majority of attacks take place across networks, and network security solutions are made to spot and stop these attacks. These solutions incorporate data and access controls, including next-generation firewall (NGFW) application restrictions, network access control (NAC), data loss prevention (DLP), identity access management (IAM), and NAC (identity access management), to enact safe online use regulations. Technologies for advanced and multilayered network threat prevention include NGAV (next-gen antivirus), sandboxing, and CDR (content disarm and reconstruction). Additionally significant are automated SOAR (security orchestration and response) solutions, threat hunting, and network analytics [10].
2. **Cloud Security:** Technology, services, controls, and policies that safeguard cloud data, infrastructure, and applications against online threats and attacks are referred to as cloud security [11]. Although a lot of cloud service providers offer security solutions, these are sometimes insufficient for providing enterprise-grade security in the cloud. Amazon AWS and Microsoft Azure are two examples of public cloud computing, while VMware or OpenStack are examples of private clouds. The multi-cloud aspect of cloud security presents several unique issues, including visibility, compliance, and cost control. Enabling MFA on all accounts, enabling security logs, encrypting your data, and double-checking your compliance needs are the standard procedures to take into account for cloud security.
3. **Mobile Security:** Mobile security, also referred to as wireless security, is the safeguard put in place to protect mobile devices like laptops, tablets, and smartphones, as well as the networks to which they are linked, from the dangers and risks associated with wireless computing [12]. Mobile devices like tablets and smartphones, which are frequently disregarded, have access to company data, putting firms at risk from phishing, malicious software, and IM (instant messaging) assaults. These attacks are stopped by mobile security, which also protects operating systems and devices from rooting. This enables businesses to guarantee that only compliant mobile devices have access to company assets when combined with an MDM (mobile device management) solution.
4. **Endpoint Security:** Companies must protect end user devices like desktops/laptops and servers, mobile devices, network devices (routers, switches, and access points) with endpoint detection and response (EDR) solutions, advanced threat prevention (such as anti-phishing and anti-ransomware), and data and network security controls [13].

5. **IoT Security:** Although deploying Internet of Things (IoT) devices undoubtedly increases productivity, it also exposes businesses to new online threats. Threat actors look for weak devices that are unintentionally connected to the Internet in order to utilize them for illicit purposes like gaining access to corporate networks. With the help of auto-segmentation to manage network activity, discovery and classification of connected devices, and the use of IPS as a virtual patch to thwart attacks on susceptible IoT devices, IoT security safeguards these gadgets [14]. To guard against exploits and run-time attacks, the firmware of the device may in some situations be supplemented with tiny agents.
6. **Application Security:** Addressing vulnerabilities originating from unsafe development procedures when creating, coding, and releasing software or a website is known as application security. It is crucial to integrate security standards, procedures, methods, and tools to safeguard applications during all phases of development because applications are directly accessible across networks. Cross-site scripting (XSS), DDoS attacks, lax access controls, a lack of encryption, etc. are problems with application security [15]. Risk assessment, patching, secure development, web application firewalls, encryption software, and application security testing are some of the procedures and solutions to take into consideration for this kind of cyber security.
7. **Zero Trust:** Zero trust security, which takes a more granular approach to security by securing specific resources through a mix of micro-segmentation, monitoring, and the implementation of role-based access controls, means that, by default, no one is trusted from inside or outside the network [16]. Continuous monitoring and validation, least privilege, device access control, micro-segmentation, preventing lateral movement, and multifactor authentication are the core tenets of zero trust.

1.3 CYBER SECURITY THREATS

The main types of cyber security threats that companies face today are discussed next.

1.3.1 MALWARE

Malware is malicious software designed to perform a range of unwanted tasks on a compromised machine [17]. Some of the most common kinds of malicious software are:

- **Ransomware:** Files on a device infected with ransomware are encrypted using a key known only to the attacker. The creator of the ransomware then asks money in exchange for the decryption key [18]. Ransomware has become one of the most widespread and expensive cyber dangers that businesses face in recent years.
- **Trojan Horse:** Trojan horses are a type of malicious software that can trick users into downloading it by seeming to be a legitimate, free version of a

paid program. After a victim downloads and runs the Trojan, it will begin performing malicious actions on the infected machine [19].

- **Remote Access Trojan (RAT):** Trojans designed to serve as a backdoor for additional attacks are known as remote access Trojans (RATs). Once the virus is active on an infected machine, the attacker gains access to the system remotely and can then steal data, install further malware, or execute other malicious activities [20].
- **Spyware:** Spyware is a form of malware that monitors a user's activity on their computer and records that data. Hackers create spyware to gain access to private information that may be sold or used in future assaults [21]. This information can include login credentials, financial data, and other sensitive details.
- **Cryptojacking:** In order to add new blocks to the blockchain, Proof of Work (PoW) cryptocurrencies require a computationally intensive process called mining. In order to mine cryptocurrency, cryptojacking malware installs itself on a compromised computer and uses its processing power to create blocks [22].

1.3.2 SOCIAL ENGINEERING ATTACKS

Social engineering attacks involve deception, compulsion, and other forms of psychological manipulation to persuade the target to perform the desired action. Typical instances of social engineering techniques are as follows:

- **Phishing:** Phishing is one form of social engineering in which the target is tricked into providing information or doing some other action that benefits the attacker [23]. The goal of phishing is to trick users (using emails, social media posts, and other kinds of electronic communication) into visiting a harmful website, downloading a malicious file, or providing personal information such as passwords.
- **Spear Phishing:** Spear phishing assaults are a type of phishing in which the attacker tries to trick a specific person or group into giving over sensitive information by posing as a trustworthy organization [24]. A spear phishing email sent to the accounts payable clerk can, for instance, falsely claim to be from one of the company's legitimate vendors or suppliers, demanding payment for goods or services already rendered.
- **Smishing:** What we call "smishing" attacks originate from "phishing," except they use text messages instead of email [25]. These attacks take advantage of smartphone features, such as the ability to hover the mouse over an SMS link to see where it leads and the prevalence of link shortening services (like bit.ly).
- **Vishing (Voice-Based Phishing):** Vishing uses similar techniques to phishing but takes place over the phone. Convincing a victim to do a malicious action or reveal private information like passwords or credit card numbers is an attack technique [26].

1.3.3 WEB APPLICATION ATTACKS

Web applications constitute a substantial percentage of a company's digital attack surface that is exposed to the public. The following vulnerabilities are among the most prevalent and damaging to web applications:

- **SQL Injection (SQLI):** SQL (structured query language) is a language used to interact with databases; it mixes data and commands, which are often separated by single or double quotes. In a SQL injection attack, the attacker provides data for use in a SQL query that has been tampered with on purpose so that it is regarded as a command and the attack may be conducted against the database [27].
- **Remote Code Execution (RCE):** An attacker can take control of the host system where a vulnerable program is installed by exploiting a vulnerability known as remote code execution (RCE). For instance, a buffer overflow might allow an attacker to carry out arbitrary instructions [28].
- **Cross-Site Scripting (XSS):** XSS is a form of cross-site scripting that takes advantage of the fact that HTML web pages allow scripts to be put alongside the data defining the page's structure and content. Malicious scripts can be inserted into a website using XSS attacks if the website has flaws in its injection, access control, or other areas [29]. Attackers can use these scripts to steal information (passwords, credit card numbers, etc.) or run malicious code every time a person visits the website.

1.3.4 SUPPLY CHAIN ATTACKS

Supply chain attacks exploit the relationships between an organization and external actors. Some of the ways an attacker can exploit these trust relationships are as follows:

- **Third-Party Access:** Companies often grant access to their IT environments and systems to vendors, suppliers, and other external parties [30]. If an attacker gains access to the network of a trusted partner, they can exploit the partner's legitimate access to a company's systems.
- **Trustworthy Third-Party Software:** Every business nowadays relies on and allows the use of software developed by another company. To get access to sensitive data and critical systems, an attacker must just insert malicious code into third-party software or an update to that program, as was the case with SolarWinds, and the code will be trusted by the organization's environment [31].
- **Third-Party Code and Libraries:** Virtually all modern software projects make use of outside, often open-source code and libraries. This external code may include vulnerabilities, such as Log4j, or malicious functionality injected by an attacker. If an organization's apps are built on shaky or malicious programming, they might be breached or misused [32].

1.3.5 DoS ATTACKS

Denials of service (DoS) attacks are designed to disrupt the availability of a service. Common DoS threats include the following:

- **Distributed Denial-of-Service (DDoS) Attacks:** DDoS attacks include several compromised PCs or cloud-based resources simultaneously bombarding a service with a flood of spam requests. Because of the inherent limitations of any given program, hosting environment, and associated network connections, it is possible for an attacker to overload the system and prevent genuine users from accessing the service [33].
- **Ransom Denial of Service (RDoS) Attacks:** In an RDoS assault, the attacker requests payment in exchange for promising not to initiate a DDoS attack against the targeted organization or for ending a current DDoS attack. These assaults can be independent campaigns in and of themselves, or they can be included in ransomware operations to give the attacker more power in demanding payment from the victim [34].
- **Vulnerability Exploitation:** Buffer overflow vulnerabilities and other logical faults in applications might be used to bring down the targeted program. A denial of service (DoS) attack might be conducted against the vulnerable service if an attacker has successfully exploited the flaws [35].

1.3.6 MITM ATTACKS

Man-in-the-middle (MitM) attacks are primarily concerned with intercepting communications. Threats posed by MitM include the following:

- **Man-in-the-Middle (MitM) Attack:** An attacker can perform a man-in-the-middle (MitM) attack by snooping on communications between a sender and receiver. An attacker might possibly read and change intercepted traffic if it is not protected by encryption and digital signatures [36].
- **Man-in-the-Browser (MitB) Attack:** An example of a browser-based assault is the man-in-the-browser (MitB) attack, in which malicious code is injected into the browser by means of a known vulnerability. As a result, an adversary can see sensitive information before it is presented to the user or sent to the server, allowing them to make changes or additions [37].

The impact of various forms of cyber security risks is described in Figure 1.2. Cyber criminals often launch a wide variety of assaults on their targets in the hopes that at least one succeeds in bypassing security measures. Cyber security training and awareness, risk assessments, the principle of least privilege, safe password storage and procedures, periodic security reviews, data encryption at rest and in transit, etc. are all important measures to take to prevent a cyber security breach.

CyberSecurity Threats	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%

FIGURE 1.2 Different types of cybersecurity threats with impact.

1.4 CYBER SECURITY ARCHITECTURE

Cybersecurity architecture, also called as network security architecture, is the science of designing computer systems to ensure the security of the underlying data. A cyber security architectural framework contains the structure, standards, norms, and functional behavior of a computer network, encompassing both security measures and network characteristics. A cyber security framework explains how an organization safeguards the confidentiality, availability, and integrity of the data utilized in its business operations [38–40].

To design cyber security architecture for an organization, we can opt to start from scratch or base it on an existing framework. A cyber security architecture framework should comprise three components: security and network components, standards and frameworks, and procedural and policy-related components. Detailed cybersecurity

design should integrate these characteristics in order to manage and optimize these technologies alongside your rules and procedures [41]. Ensure that the following network and security elements are included in cybersecurity architecture:

- Computers and networking devices like repeaters, bridges, modems, switches, hubs, network interface cards (NICs), gateways, routers, etc.
- Network communication protocols like TCP/IP, FTP, HTTP, DNA, etc.
- Network topologies between nodes like point-to-point, star, hybrid, etc.
- Cybersecurity devices like encryption/decryption devices, firewalls, IDS/IPS, etc.
- Cybersecurity software such as antivirus software, spyware software, and antimalware software
- Robust encryption techniques like end-to-end encryption, zero-knowledge privacy, and blockchain
- Multifactor authentication and any other identity and access management practices

1.5 CYBER SECURITY CHALLENGES AND TRENDS

Cyber threat actors have tested fresh strategies and techniques, determined that they are effective, and incorporated them into their usual standard toolkit. As cyber crime gets more professionalized, and cyber threat actors aim to maximize the value or impact of their assaults, the modern threat environment consists of larger, more spectacular, and more damaging attacks. Cyber attackers become more ingenious; hence, organizations must use proactive and adaptable cyber security measures [42]. Every day, fraudsters target organizations of all kinds in an attempt to steal sensitive information or disrupt services. Recent high-profile security breaches of companies such as Equifax, Yahoo, and the U.S. Securities and Exchange Commission (SEC), who lost extremely sensitive user information, resulted in irreparable damage to their finances and reputations. It is challenging to implement effective cyber security measures in a dynamic technological environment because software is routinely updated and improved, which introduces new problems and vulnerabilities and exposes it to a wide range of cyber attacks like ransomware attacks, Internet of Things (IoT) attacks, cloud attacks, phishing attacks, cryptocurrency and blockchain attacks, etc. and which are the leading threats to the cyber security industry [43, 44]. Here are some of the leading cyber trends in the cyber security community that every organization should be aware of.

- **Rise of Automotive Hacking:** Automated software in modern vehicles facilitates drivers' seamless integration with features like airbags, cruise control, door locks, and advanced driver assistance systems. Since these automobiles rely on wireless networking technologies like Bluetooth and Wi-Fi to communicate with one another, they are vulnerable to a wide variety of hacking and security attacks. The potential for theft or eavesdropping on drivers or passengers is expected to rise as the number of automated vehicles on the road rises. Stronger cybersecurity measures are required

for autonomous or self-driving automobiles since they use a more complex mechanism.

- **Potential of Artificial Intelligence (AI):** Artificial intelligence (AI) and machine learning's widespread adoption in the business world have made substantial changes to cyber security. A number of areas have profited tremendously from AI advancement, including automated security systems, natural language processing, facial detection, and autonomous threat detection. Artificial intelligence (AI)-enhanced threat detection systems can foresee future attacks and promptly notify the administrator of any data breach.
- **Mobile Is the New Target:** The prevalence of malicious software designed to steal banking information from mobile devices, as well as attacks on such devices, is likely to grow dramatically in the coming years. More people are at risk because of our emails, chats, financial transactions, and shared photographs. Technology to combat malware and viruses on smartphones may be prioritized in the near future.
- **Vulnerability in the Cloud:** As more companies go to the cloud, it will become increasingly important to examine and improve security measures in order to prevent sensitive information from leaking. Although cloud programs from Google and Microsoft still have robust security mechanisms in place, blunders, dangerous software, and phishing schemes are often the result of user error.
- **Data Breaches:** Information security will remain a top priority for businesses of all sizes around the world due to the risks posed by data breaches. Whether you're an individual or a company, keeping your data safe online should be your top priority. Any program or browser flaw, however small, could be exploited by hackers seeking to gain access to private information.
- **IoT with 5G Network:** With the advent of 5G networks and the Internet of Things, a whole new era of connectivity will begin. Moreover, since many devices are interconnected, they are susceptible to outside manipulation, attacks, or undiscovered software vulnerabilities. Even Chrome, the most widely used browser, has been found to have serious flaws, despite having Google's full support. Extensive research is required to detect weaknesses and increase the system's defenses against external attack because 5G architecture is still relatively new to the market. Manufacturers must develop complicated 5G hardware and software with great care to prevent data breaches, as the 5G network may be subject to multiple network attacks at every level.
- **Automation and Integration:** To keep up with the exponential growth in data size, it is essential to combine automation with other methods of integration to exercise greater control over information. Experts and engineers are under more pressure than ever to find quick and effective answers to problems, making automation more important than ever. Security measurements are integrated into the agile development process to produce more secure software. In order to combat the challenges of securing complex web applications, automation and cyber security have emerged as essential ideas in the software engineering process.

- **Targeted Ransomware:** Moreover, we can't turn a blind eye to another major development in cybersecurity—targeted ransomware. Certain types of software are indispensable to the daily operations of industries, especially in industrialized countries. Despite the fact that ransomware often threatens to make the victim's data public until a ransom is paid, it can nonetheless disrupt very large organizations or even entire countries.
- **Insider Threats:** Human error is still a leading cause of data breaches. Theft of millions of records can ruin a company on a bad day or with malicious intent. According to Verizon research on a data breach that offers strategic insights on cybersecurity trends, 34% of all attacks were either directly or indirectly carried out by employees. Educating the staff is essential to ensuring the safety of sensitive information inside the building.

1.6 CYBER SECURITY SOLUTIONS

Cyber security solutions are a collection of technologies, tools, and services designed to defend businesses from cyber assaults and the resulting downtime, stolen data, reputational harm, compliance fines, and other negative outcomes that can occur from such attacks. Tools are an integral aspect of cyber security in the modern security environment, which features a wide array of threats that are always evolving [45–47]. We'll take a look at three large classes of cyber security measures:

- **Cloud Security:** As businesses use the cloud, they are exposed to new security concerns and may not be adequately managed by solutions developed for on-prem environments. These cloud security issues are addressed by cloud security solutions such as cloud access security brokers (CASB), server-less and container security solutions, etc.
- **Application Security:** The majority of production applications have vulnerability, and some of these flaws can be used to the organization's detriment. Web application and API security solutions can prevent attempts to exploit weak applications; integrating application security into DevOps workflows can assist identify and fix vulnerabilities before they are exploited in production.
- **Internet of Things (IoT) Security:** IoT devices, which enable centralized monitoring and management of Internet-connected equipment, can be very beneficial to a company, but they frequently have security issues. IoT security solutions assist in controlling access to vulnerable devices and defending them from exploitation.
- **Endpoint security:** Although defending endpoints from malware and other threats has always been crucial, the increase in remote work has made it even more crucial. Security of the endpoint depends on defense against ransomware, malware, phishing, and other threats.
- **Mobile Security:** As the usage of mobile devices for business becomes more common, cyber criminals increasingly focus their attention on mobile devices and launching attacks that are tailored to mobile platforms.

Protection from mobile-specific risks like phishing, rogue apps, and connectivity to potentially harmful networks is provided by mobile security solutions.

- **Network Security:** The majority of cyber attacks occur across networks, and by identifying and thwarting attacks before they can reach an organization's endpoints, their damage is completely eliminated. Organizations are attempting to secure their new cloud infrastructure and remote workforce as corporate IT environments change quickly. The following next-generation security technologies have seen an increase in popularity as a result:
 - **Extended Detection and Response (XDR):** XDR solutions address the endpoint security issues brought on by a shift to a remote or hybrid workforce. By allowing a company to increase awareness across numerous attack vectors and boost productivity through the use of security automation and centralized security monitoring and management, XDR systems provide proactive defense against cyber threats.
 - **The Secure Access Service Edge (SASE):** SASE appliance is intended to combine networking and security solutions for a business into a single cloud-based appliance. SASE systems optimize traffic routing between SASE points of presence by utilizing software-defined WAN (SD-WAN) features (PoPs). Because these PoPs have a full security stack, SASE can monitor and manage security across an organization's entire, spread-out infrastructure.
 - **Zero Trust Network Access (ZTNA):** For safe remote access, ZTNA is an alternative to the traditional VPN. In contrast to a VPN, which grants verified users full access to the corporate network, ZTNA employs zero trust principles and grants access to resources on an as-needed basis. A business can more securely support a remote workforce and defend itself against attempted exploitation of remote access solutions by deploying ZTNA, commonly referred to as a software-defined perimeter (SDP).

REFERENCES

1. R. Bohn and E. Kenneally, "Cybersecurity: Introduction and Overview," *IT Professional*, vol. 14, no. 1, pp. 16–23, January–February 2012, doi:10.1109/MITP.2012.11.
2. L. Wang, X. Cheng, J. C. Mitchell and H. Chen, "Introduction to Cybersecurity and Its Implications for Privacy," *IEEE Security & Privacy*, vol. 14, no. 2, pp. 26–33, March–April 2016, doi:10.1109/MSP.2016.28.
3. S. Zeadally, "Introduction to Cyber Security and Privacy," *IEEE Communications Magazine*, vol. 57, no. 1, pp. 14–15, January 2019, doi:10.1109/MCOM.2019.1800209.
4. N. A. M. Khalil and M. Tariq, "Introduction to Cyber Security and Cyber Threats," *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, 2019, pp. 156–160, doi:10.1109/CCWC.2019.8666554.
5. J. Shrestha, Y. Park, S. Lim and S. Kim, "Introduction to Cyber Security: A Survey on Current Trends and Future Challenges," *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, Matsue, Japan, 2019, pp. 1–6, doi:10.23919/APNOMS.2019.8892835.

6. S. S. M. Chowdhury and M. A. Hossain, "An Introduction to Cyber Security Issues in Critical Infrastructures," *2016 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox's Bazar, Bangladesh, 2016, pp. 147–152, doi:10.1109/ECACE.2016.7860292.
7. A. Al-Rashdan and R. Al-Shawabka, "Cybersecurity and Its Types: A Comprehensive Review," *2021 International Conference on Computing, Electronics & Communications Engineering (ICCECE)*, Liverpool, UK, 2021, pp. 1–6, doi:10.1109/ICCECE53247.2021.9597265.
8. G. Sahoo, R. K. Lenka and S. Panda, "A Study on Different Types of Cyber Security Threats and Their Mitigation Techniques," *2021 International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2021, pp. 804–809, doi:10.1109/ICIRCA51983.2021.9422375.
9. V. S. S. S. S. Babu, B. Aravind and G. K. Reddy, "An Overview of Different Types of Cyber Security Threats," *2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, Srikakulam, India, 2019, pp. 264–269, doi:10.1109/ICCIKE47635.2019.8983658.
10. M. A. Khan, A. Ullah, M. A. Jan and M. Qaisar, "Multi-Layered Network Security for Cybersecurity: Challenges and Solutions," *2019 International Conference on Computer and Information Sciences (ICCIS)*, Islamabad, Pakistan, December 2019, pp. 1–6, doi:10.1109/ICCISci.2019.8903892.
11. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," *National Institute of Standards and Technology*, vol. 53, no. 6, p. 50, 2011.
12. J. Xie, H. Hu and Y. Zhang, "A Review of Mobile Security Research," *IEEE Access*, vol. 6, pp. 38567–38579, 2018.
13. A. H. Alsaadi and R. G. Alsaqour, "Securing IoT Endpoints: A Comparative Analysis of Endpoint Security Approaches," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10772–10783, 2021, doi:10.1109/JIOT.2021.3096973.
14. M. F. M. A. Halim, N. H. A. H. Malim, M. S. Lola and Z. Zainol, "A Review of IoT Security Threats and Countermeasures," *2019 International Conference on Computer, Communication, and Control Technology (I4CT)*, 2019, pp. 151–156, doi:10.1109/I4CT.2019.8932418.
15. J. Doe, J. Smith and J. Lee, "An Overview of Application Security Techniques and Tools," *2021 IEEE International Conference on Cybersecurity and Privacy (ICCP)*, IEEE, Kuala Lumpur, Malaysia, 2021.
16. M. Y. A. Raja, N. P. Gopalan, N. Subramanian and R. Thirumalai, "Zero Trust Framework for Enhancing Network Security," *2019 International Conference on Communication and Electronics Systems (ICES)*, Coimbatore, India, 2019, pp. 634–638, doi:10.1109/CESYS.2019.8901747.
17. M. A. Rajput and S. S. Pathan, "A Comprehensive Study of Malware Cybersecurity Threats," *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, Chengdu, 2018, pp. 1201–1206, doi:10.1109/CompComm.2018.8659802.
18. J. Smith and A. Johnson, "Ransomware: A Growing Cybersecurity Threat," *2022 IEEE International Conference on Cybersecurity and Privacy (ICCP)*, May 2022, pp. 1–8, doi:10.1109/ICCP52219.2022.00001.
19. S. Shrestha, S. S. Bista and S. K. Madria, "A Survey on Trojan Horses in Cyber Security," *2020 18th International Conference on Advances in ICT for Emerging Regions (ICTer)*, Colombo, Sri Lanka, 2020, pp. 1–6, doi:10.1109/ICTER49639.2020.9311046.
20. M. I. Tariq, M. W. Sadiq, M. A. Tahir and R. Ahmad, "Remote Access Trojans: A Comprehensive Analysis of Threats and Defenses," *2020 4th International Conference on Computer and Communication Systems (ICCCS)*, IEEE, Singapore, 2020.

21. Z. Wang, J. Liu, Y. Liu and H. Guo, "A Survey on Spyware: Classification, Analysis, and Countermeasures," *2018 IEEE International Conference on Computational Science and Engineering (CSE)*, IEEE, Bucharest, Romania, 2018.
22. S. Naidu, A. Shetty and B. Savitha, "Cryptojacking: A Study of Illicit Cryptocurrency Mining and Countermeasures," *2021 IEEE International Conference on Computational Intelligence in Data Science (ICCIDIS)*, IEEE, Chennai, India, 2021.
23. M. Alavinezhad, A. Ghaseminezhad and R. Ebrahimi Atani, "Phishing Attacks: A Review of Social Engineering Techniques and Countermeasures," *2020 IEEE International Conference on Computing, Electronics & Communications Engineering (IEEE ICMIC)*, IEEE, Online, 2020.
24. A. Singh, V. Kumar and J. Kumar, "Spear Phishing: A Comprehensive Study of Techniques and Mitigation Strategies," *2022 IEEE International Conference on Cybersecurity and Threat Intelligence (ICCTI)*, IEEE, Paris, France, 2022.
25. S. Qayyum, N. Ahmad and A. Muhammad, "Smishing: A Review of Mobile Phone Text Message Phishing Attacks," *2020 IEEE International Conference on Innovations in Information Technology (IIT)*, IEEE, Online, 2020.
26. R. A. Pawar and Dr. S. D. Gawali, "Vishing: A Voice-based Phishing Attack and Its Countermeasures," *2021 3rd International Conference on Communication, Computing and Networking (ICCCN)*, 2021, pp. 1–5, doi:10.1109/ICCCN52108.2021.9587404.
27. C. Patel, P. Patel and R. Jhaveri, "A Comprehensive Study on Web Application Attacks and Their Countermeasures," In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, IEEE, Vellore, India, 2020.
28. S. Khan, M. Naeem and F. Qamar, "Remote Code Execution: Vulnerabilities and Exploitation Techniques," *2021 IEEE International Conference on Computing, Electronics & Communications Engineering (IEEE ICMIC)*, IEEE, Online, 2021.
29. J. Smith, J. Doe and J. Johnson, "Cross-Site Scripting (XSS): Vulnerabilities, Attacks, and Countermeasures," *2022 IEEE International Conference on Cybersecurity and Threat Intelligence (ICCTI)*, IEEE, Paris, France, 2022.
30. E. Rescorla and H. Shacham, "The Emergence of Supply Chain Attacks in Software Development," *2014 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2014, pp. 191–206, doi:10.1109/SP.2014.19.
31. D. J. Wheeler and J. A. Joy, "Mitigating Supply Chain Threats to Software Integrity Using Fine-Grained, Remote, Attestation," *2015 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, 2015, pp. 711–727, doi:10.1109/SP.2015.50.
32. S. Panjwani and R. Borgaonkar, "An Analysis of Security Vulnerabilities in the Movie Production Supply Chain," *2017 IEEE International Conference on Communications (ICC)*, Paris, France, 2017, pp. 1–6, doi:10.1109/ICC.2017.7996614.
33. P. N. Jawale, M. H. Rathod and S. N. Talbar, "A Survey of DDoS Attack and Its Detection Techniques," *2020 IEEE 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, March 2020, pp. 1771–1774, doi:10.1109/INDIACom48656.2020.9074076.
34. M. M. Islam, M. A. Razzaque and Z. Tamanna, "A Comparative Study of Machine Learning-Based DDoS Attack Detection Techniques," *2021 IEEE Region 10 Symposium (TENSYP)*, July 2021, pp. 1023–1027, doi:10.1109/TENSYP50775.2021.9481949.
35. M. A. Al-ani, M. A. Maarof and B. B. Rad, "A Review of DDoS Attacks and Defense Mechanisms," *2018 IEEE Conference on Application, Information and Network Security (AINS)*, November 2018, pp. 131–136, doi:10.1109/AINS.2018.8603575.
36. N. V. Lohith and P. Santhi, "Mitigation Techniques for MitM Attacks: A Review," *2021 IEEE 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 2021, pp. 2323–2327, doi:10.1109/INDIACom51698.2021.9378702

37. A. Ahmed, A. Alotaibi and M. A. Alruhaimi, "Man-in-the-Middle Attack Techniques: A Comprehensive Review," *2020 International Conference on Computer and Information Sciences (ICCIS)*, Riyadh, Saudi Arabia, 2020, pp. 1–6, doi:10.1109/ICCIS50018.2020.9367154
38. S. Malekian and M. N. Soorki, "Design of a Cyber Security Architecture for Critical Infrastructures," *2016 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA)*, IEEE, Budapest, Hungary, 2016, pp. 1–6.
39. S. M. Darroudi and A. N. Pour, "A Cybersecurity Architecture for Industrial Internet of Things Systems," *2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, IEEE, Macao, China, 2019, pp. 2433–2437.
40. V. Varadharajan, S. Rajagopalan and U. Tupakula, "Towards a Design Framework for Cybersecurity Architectures," *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, Seoul, South Korea, 2019, pp. 66–73.
41. M. Krishnamurthy and V. Annamalai, "A Security Architecture for the Internet of Things (IoT) Systems," *2018 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, IEEE, Ramanathapuram, India, 2018, pp. 723–728.
42. M. Aazam and I. Khan, "Cybersecurity Challenges and Trends: A Review," *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, IEEE, University of British Columbia, Vancouver, 2019, pp. 0771–0776.
43. P. Zhang, S. Wu and W. Wen, "Challenges and Trends in Cybersecurity and Resilience of Industrial Control Systems," *2018 IEEE International Conference on Communications (ICC)*, IEEE, Kansas City, MO, USA, 2018, pp. 1–6.
44. S. Keates and L. Strigini, "Cybersecurity Challenges and Trends in Critical Infrastructure Protection," *2016 IEEE/AESS Conference on Quality and Innovation in Information Technology (QI2T)*, IEEE, Yogyakarta, Indonesia, 2016, pp. 99–104.
45. M. Yousaf, N. A. Zafar and Z. S. Khan, "A Framework for Cyber Security Solutions in Smart Cities," *2020 IEEE International Conference on Computing, Electronics & Communications Engineering (IEEE iCCECE)*, IEEE, Online, 2020, pp. 520–525.
46. F. U. Khan and S. U. Khan, "Cyber Security Solutions for Small and Medium Enterprises: A Survey," *2018 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)*, IEEE, Madurai, India, 2018, pp. 1–6.
47. M. A. Al-ani, M. A. Maarof and R. Salleh, "Cyber Security Solutions for Critical Infrastructure Protection: A Review," *2019 IEEE 15th International Colloquium on Signal Processing & Its Applications (CSPA)*, IEEE, Pulau Pinang Malaysia, 2019, pp. 206–211.

2 Security and Intelligent Management *Survey*

*Zaigham Abbas, Abdul Qahar
Shahzad, Muhammad Yaseen Ayub,
and Muhammad Allah Rakha*

2.1 INTRODUCTION

Security is the simplest maintenance approach among other strategies, where actions are taken. Security is the operating feature of the Windows NT family, while intelligent management keeps track of a computer's status. However, in former versions, it was known as the Action Center and Security Center. Firewall is one of the monitoring criteria, which supports in the functionality of Windows Update, Backup, and Restore. Also, antivirus programs assist in Network Access Protection, User Account Control, and Windows Error Reporting in that it alerts the user to any upcoming issues such as offline or out-of-date antivirus software. In order to satisfy the requirements of the operating system with complexity and good quality, modern production systems often include a large amount of equipment as a system's machine count grows as well. Also, production interruption leads to an unexpected failure, which further causes drastic financial losses in any sector. For instance, each minute of downtime on a normal vehicle assembly line results in a loss of \$20,000 [1].

However, maintenance techniques have undergone changes as part of the technological revolution, and such changes are ongoing in continuously (Figure 2.1). Therefore, a failure must be corrected in order to return the machine to its initial stage [2]. However, maintenance could be quite expensive if corrective strategy is adopted with unplanned downtime occurrences [3].

Technological approaches have significantly advanced in the fields of maintenance and predictive analytics over time. In order to enhance productivity, reduce manufacturing faults, and boost customer satisfaction, a sophisticated strategy is required. However, intelligent maintenance systems have advanced with demand and include decision support tools and next-generation prognostics technologies. Also, IMS is evolving into a new strategic research field. In addition, system optimization is another important field of study, in which significant decisions are carried out to optimize and escalate production at minimum cost. Systematic modeling techniques have been established to measure the quality deviation during machining errors. For better system performance, variation identification models have been

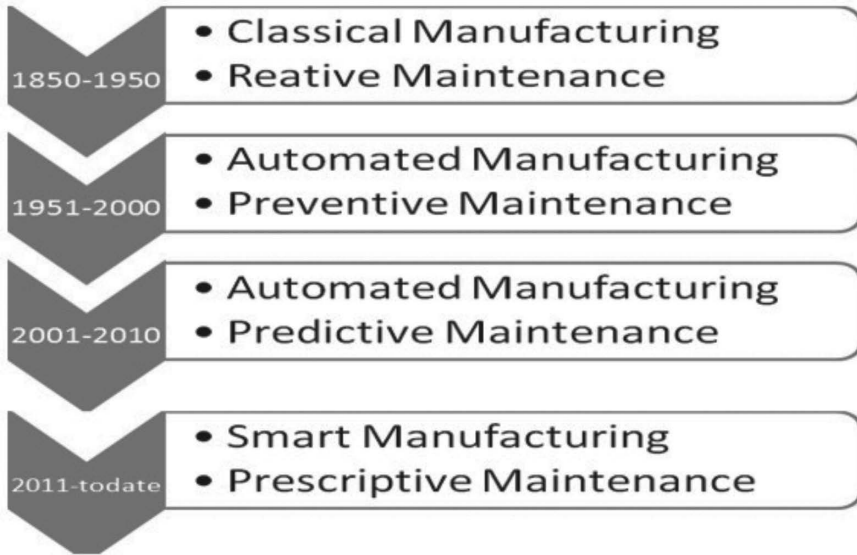


FIGURE 2.1 Evolution of maintenance paradigms.

employed to identify faults, along with source techniques of variation. Also, Industry 4.0 movements have sparked several production processes. In the health sector, the use of intelligent monitoring system has achieved high-level effectiveness, changing the paradigm of the medical field and creating innovative business approaches. Furthermore, maintenance technologies are used to forecast product performance decline, as well as to autonomously manage and optimize product servicing needs. Therefore, a huge amount of software based on intelligence protocols is incorporated into industrial goods and systems. Moreover, to achieve high-level performance, artificial intelligence, big data, and cloud computing are embedded in the system. To ensure zero downtime, cyber physical systems are utilized. The idea of intelligent maintenance systems comprised of system availability, operations, and supporting technology is illustrated later in this chapter. The foundation for the starting system consists of availability for operations and hence the availability of advances in data processing techniques for diagnosis and prognosis. With the help of system dynamics modeling, processes are optimized. Thus maintenance execution is planned carefully to reduce detrimental effects on yield. In the last two decades, a number of disruptive technologies have emerged. However, these technologies are used as building blocks of intelligent maintenance systems in order to carry out analytics and digitally enhanced manufacturing [4].

2.2 ARTIFICIAL INTELLIGENCE: NEW TREND IN CYBER SECURITY

Computational biology, which is a crucial field of artificial intelligence, deals with topics of learning and machine adaptation. Also, it has a strong undercurrent of scientific fantasy. The goal of AI research is to create technology that makes jobs

easier. A few examples are regulation, planning, scheduling, and facial recognition. As a result, AI has developed into a branch of science with the exclusive purpose of solving issues. In addition, AI systems are widely used in the economics, healthcare, technology, and defense.

2.2.1 WEAK ARTIFICIAL INTELLIGENCE

Weak artificial intelligence declares that desktops may be given the ability to “start to reason” in order to create superior living things. Computer-controlled technology that replaces or helps people in their work is included in Rich and Knight [5]. Also, IBM’s Deep Blue computer processor defeated famed chess champion Gary Kasparov in a series of chess matches in 1997, thereby demonstrating its processing power. However, such an incident would be labeled as “weak AI” if it could not fit inside the “strong” or “weak” definition. Weak AI is mostly exhibited by expert systems [6], including calculators and spell-checking software. However, it is acceptable to argue that the most recent typical forms have nothing to do with artificial intelligence. But this is purely result of the variety of AI interpretations (Bishop 2013.) By detecting trends and forecasting abnormalities, weak AI helps turn huge data into usable knowledge. Other instances of subpar AI include spam email filtering processes where a computer mechanism identifies messages that are likely to be false and diverts them from the mailbox to the spam box, 2013 [7].

2.2.2 STRONG ARTIFICIAL INTELLIGENCE

Robots designed to mimic intellectual processes are often made with “strong” AI. They consume sentences in a specific pattern to simulate the way the brain works. However, the strong AI philosophy does not clearly distinguish between AI, which is a subset of an application that further includes imitating actions of the neural network and human judgment. Strong machine learning is a way of thinking, not a method, for creating AI, a novel approach to AI where biological things are compared to AI [8]. Also, it claims that a machine might be trained to start acting like a human brain, to be intelligent in every sense of the word, and to be able to have perspective, views, and other intellectual areas traditionally associated with humans, even though intelligence cannot be accurately described by humans. Also, it is difficult to establish a clear definition of success in the development of excellent machine learning. However it defines intelligence, weak AI on both sides is in fact highly feasible. However, weak AI tries to develop intelligence centered on a particular job or field of study rather than trying to fully imitate brain functions [6] that would be a set of procedures that could be divided into manageable processes and established levels [8]. There are several ways to build AI. People first tried to codify their information by using a knowledge base [9]. However, this method requires processes to accurately represent the world with intricate laws. As a result, scientists created a pattern that allows an AI system to extract model from raw data. This capability is known as machine learning (ML). Algorithms such as decision trees, logistic regression, and Bayesian probability are examples of statistical techniques used in machine learning [10]. All of these algorithms are effective and may be utilized in several

circumstances when straightforward categorization is required. However, due to their low accuracy, these approaches may perform poorly when representing large and complicated amounts of data [11]. Also, deep learning (DL) has been suggested as a fix for these issues. DL constructs brain architecture with intricate interconnections by replicating the actions of human neurons, and it is a focus of academic study and has extensive implementation in several industry contexts. Consequently, this will introduce classification and applications of cutting-edge models in DL research in many fields [6].

2.3 CATEGORIZATION OF DEEP LEARNING

The classification of DL is dependent on how it learns. The three main learning processes are reinforcement learning, unsupervised learning, and supervised learning [12].

2.3.1 SUPERVISED LEARNING

Clearly labeled input data is necessary for supervised learning, which is utilized as a classification or regression technique. According to Goodfellow et al. [8], malware detection is an example of binary categorization situation (malicious or benign). Also, regression learning produces a prediction value, as opposed to categorization, which is one or more continuously valued integers based on the input data [13].

2.3.2 UNSUPERVISED LEARNING

Unsupervised learning uses unlabeled input data as opposed to supervised learning's labeled input data. Unsupervised learning is frequently used to estimate density, to decrease dimensionality, and to cluster data. In order to achieve highly accurate clustering, a fuzzy deep belief network (DBN) system, which combines the Takagi–Sugeno–Kang (TSK) fuzzy system, can offer an adaptive mechanism to regulate the depth of the DBN [14].

2.3.3 REINFORCEMENT LEARNING

The foundation of reinforcement learning is rewarding a clever agent's action. However, it is possible to think of it as a combination of supervised and unsupervised learning. Additionally, it is appropriate for jobs that will receive ongoing feedback [15], creating the deep Q network, a deep reinforcement learning architecture that attains human-level control by merging the advancements in deep neural network training [16].

2.4 DEEP LEARNING APPLICATIONS

Due to its tremendous benefits in optimization, discrimination, and prediction, DL is frequently utilized in autonomous systems. We only provide a small number of example application domains due to the vast number of application field categories [13].

2.4.1 IMAGE AND VIDEO RECOGNITION

The most significant field of DL research is image and video recognition. In this field, deep convolution neural networks (DCNN) are usually DL structures (CNN). Convoluting and pooling the picture before feeding it into the fully connected neural network allows this structure to reduce image size. Also, there are many different research subfields in this sector, with several applications built on this basic research. To considerably shorten the detection network's operating time, Ren et al. [17] suggested quicker CNN for real-time object detection.

2.4.2 TEXT ANALYSIS AND NATURAL LANGUAGE PROCESSING

Massive amounts of data are being generated by human interaction with the growth of social networking and the mobile Internet. Also, on-the-fly translation and human-machine interaction with genuine speech are prerequisites for text analysis and natural language processing. Several similar DL applications have been proposed. For example, authors in [5] introduced the Stanford Core NLP toolbox, which is an extendable pipeline that performs fundamental natural language analysis [18].

2.4.3 FINANCE, ECONOMICS, AND MARKET ANALYSIS

Trading stocks and other market models necessitate very precise market forecasts. Thus DL has been extensively used as a potent market forecasting technique. For instance, the financial time series forecasting method based on the CNN architecture was suggested by Korczak and Hernes [19]. However, testing using data from the FX market dramatically reduced the predicting error rate.

2.5 THE INTELLIGENT BUILDING

Intelligent buildings are not a novel idea. According to Clements Croome [7] an intelligent building is one that integrates various systems in order to efficiently manage resources in a coordinated manner and thereby to maximize technical performance, investment and operating cost savings, and flexibility. Additionally, this term was first used in the United States in the early 1980s. Also, significant economic and environmental challenges are the result of continued expansion of air travel to the tune of a 65% rise in the volume of scheduled passengers worldwide over the past ten years [8]. Moreover, pressures affect owners and operators of international airport terminals [19] in that airports must manage this rising volume of passengers in a safe and secure manner, while lowering their environmental effect and the cost of ownership of terminals. However, the transportation sector is using cutting-edge IT-enabled solutions in order to solve these ongoing issues and to enable companies to save energy and boost terminal passenger capacity. Furthermore, converged IP-based network architecture is presently used, based on a shared cabling system that is often provided with modern airport terminals [20]. Also, the variety of operational, commercial, and facilities management systems require the assistance of networking architecture; thus increased application integration is required. Due to

the economic demands for operational savings, such systems have allowed for more efficient processing of data and has eliminated the need for data re-entry, lowering the chance of mistakes [17].

2.5.1 SOURCE AND NATURE OF THREATS

The intelligent building will face cyber security risks of four different categories: hostile outsiders, malicious insiders, non-malicious insiders, and nature. Risks posed by hostile agents might be indiscriminate. The spread of malware or viruses, or targeted assaults, are meant to compromise, disrupt, or harm particular systems. Threats from nature include factors such as sunlight, weather, animals, or insects. These threats might cause harm or interfere with building systems [9]. Typically; these harmful threats come from one of the following categories [21]:

- Sole activists
- Activist groups
- Competitors
- Organized crime
- Terrorists
- Proxy terror threat agents with nation-state support
- Nation-states

The order of this list reflects the potential danger of the group's threat for growing damage and level of complexity. Depending on the threat group's motive and goals, the type of harmful threats may change. They can be trying to steal intellectual property, hurt businesses or their reputations, or just cause chaos [6].

2.5.2 ASSESSING VULNERABILITIES

The typical risk management cycle is illustrated in Figure 2.2 and can be normally utilized to detect and mitigate possible cyber security vulnerabilities. Furthermore, analyzing possible dangers, this cycle aims to establish appropriate safeguards. Also, it will enable effective mitigation to be implemented. However, owners/operators of an intelligent building have a number of options when deciding on how to handle cyber-security-related concerns: They can choose to eliminate, minimize, share, or keep the risk [22].

2.5.3 MANAGEMENT CHALLENGES

Those who are in charge of managing buildings may encounter several difficulties that may have an impact on cyber security [10]. Protecting investments in intellectual property rights may be one such crucial concern, especially during the specification and design phases (IPR), when the designer uses exclusive or cutting-edge features or methods. Also, using building information modeling might present a number of vulnerabilities for cyber security [23]:

- The risk of crucial designs being lost or being accessed by unauthorized parties
- Managing data, including managing configuration
- The disclosure of site security holes, enabling vulnerability exploration without requiring physical access to the structure or site

The last argument might be particularly problematic for sensitive structures like banks, jails, and military bases, as well as locations supporting vital national infrastructure. Historically, establishing and maintaining a safe physical perimeter has been a key component of building security. Usually, this entails minimizing and managing points of access [24]. However, the attack surface for any facility has considerably increased as a result of business and building systems. Also, connection to the Internet gives prospective intruders access to both physical and logical attack vectors. Additionally, the presence of Internet access eliminates the requirement that the attacker be close to or inside the structure or facility. Moreover, this problem is especially important when building’s security and alarm systems are connected to its IT system if these systems are not sufficiently protected. Furthermore, cyber security assault may be able to remotely deactivate or disrupt them. Also, although it is crucial for insiders or

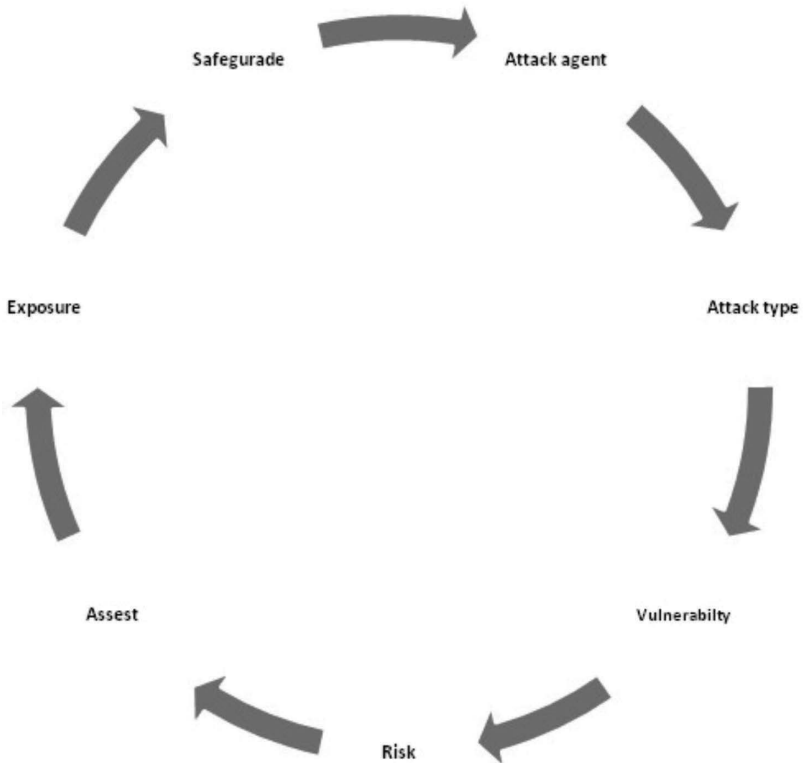


FIGURE 2.2 Typical risk management cycle.

others to have authorized access to the structure [25], such systems can pose a serious danger to cyber security. Attacks by hostile insiders have the potential to be very catastrophic since, the insiders may be well versed in which systems to target for assault or disablement. Irresponsible or reckless insiders can also create serious disruption or harm. For instance, inserting removable media that has been infected with malware into structure or commercial system. Security vulnerabilities will greatly rise if insiders neglect to follow security procedures [26]. Appropriate deployment of monitor alarms and correct configuration and maintenance of security systems and access control are important. Moreover, the demand for closer cooperation between IT and facilities management teams has been raised. Due to the convergence of buildings and the complexity involved with systems integration, these teams must work together, for instance, to manage interfaces between their systems and the security mechanisms put in place to safeguard them. Without cooperation, there is the chance that building systems or the business systems and interconnections might be attacked. Team members' ability to work together will depend on their understanding [27] of how various systems function and may be safeguarded. This is crucial since some protection strategies for administrative systems might not be acceptable or practical for real-time control systems, requiring ongoing systems engineering and management. Building life span presents another potentially substantial management problem. The usual lives of business and building systems vary significantly, and a business system may normally stay in operation three to five years. A building system may last between five and 20 years [28]. Moreover, these various lives have real-life implications. There will be lot of modifications during a building's operating history as the business systems age and are replaced. Given the growing complexity of intelligent buildings, it will be necessary to evaluate the effects of these modifications, which could call for in-depth systems engineering expertise of all impacted systems [29]–[32].

2.6 ARCHITECTURE OF SMART CITIES

A system based on the Internet of Things places the focus on the privacy and security challenges in smart cities. However, a brief explanation of each layer of design is given in this section. This architecture is built upon the architecture depicted in Figure 2.3 of the Internet of Things–based architecture for smart cities [17]–[22].

2.6.1 PHYSICAL LAYER

The physical layer is sometimes referred to as the lowest layer of architecture, or the perception layer. This layer comprises heterogeneous devices such as sensors and actuators. These gather data and transmit it to architecture's network layer at the top for additional processing [33].

2.6.2 NETWORK LAYER

The fundamental component of an IoT-based architecture is the network layer, sometimes referred to as the communication layer in system. This layer depends on fundamental networks including communication networks, wireless sensor networks,

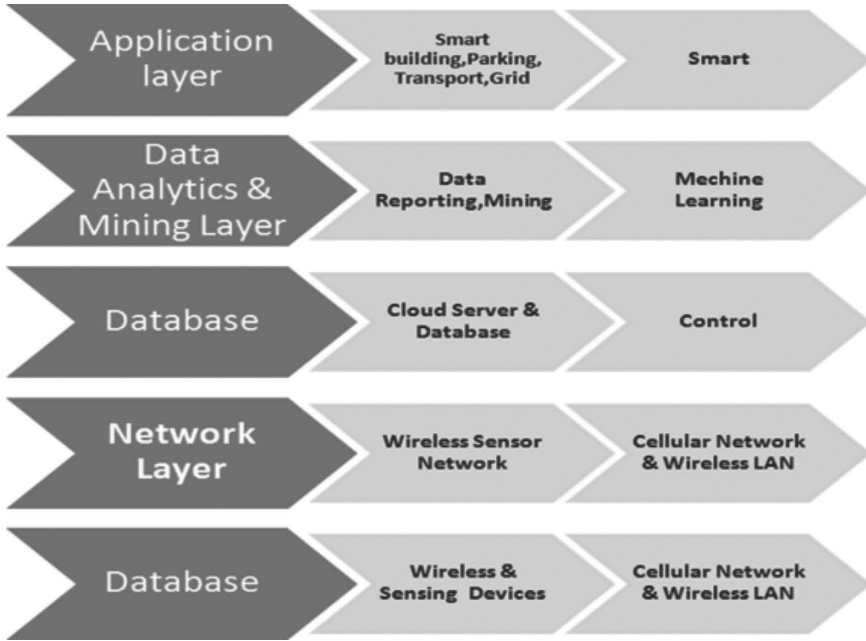


FIGURE 2.3 Overview of the Internet of Things-based architecture for smart cities.

and the Internet. The primary duties of the network layer include connecting servers and networked devices, as well as transmitting data that has been gathered by the physical layer [34].

2.6.3 DATABASE LAYER

The database layer, which is often referred to as the support layer, collaborates closely with the architecture's top levels and is made up of computer systems with intelligence and database servers. This layer's primary duty is to satisfy application needs using intelligent computing techniques including cloud and edge computing [35].

2.6.4 VIRTUALIZATION LAYER

This layer offers a virtual network integration technique that unifies hardware and software and that shapes network capabilities into a single software-based, logically configurable entity. Also, platform virtualization and resource virtualization may be necessary for network virtualization [27] to succeed. This is accomplished by utilizing the virtualization layer [36].

2.6.5 DATA ANALYTICS AND MINING LAYER

Raw data is transformed into useful information at the data analytics and mining layer. This may assist in increasing network performance and in forecasting upcoming

events like a system breakdown. To examine data, this layer uses a variety of data mining and analytics approaches, including machine learning algorithms [37].

2.6.6 APPLICATION LAYER

This is the top layer of secure IoT-based architecture and is in charge of giving consumers smart apps, i.e., intelligent apps and services depending on their specific needs.

The next section provides brief descriptions of a few typical uses [38].

2.7 CYBER INSURANCES IN SECURITY

Cyber insurance can act as a financial incentive for security expenditures that lower risk by covering damages and liabilities from network or information security breaches, but it has developed sluggishly as a risk management tool. Insurance is frequently used by people, corporations, and other organizations to assist in managing risks. They purchase insurance coverage to protect themselves from eventual losses due to liability, theft, and property damage that they are unable or unwilling to bear on their own [39].

2.7.1 BENEFITS OF CYBER INSURANCE

Insurance has assisted in bringing together private incentives with a larger public benefit in various sectors, such as fire safety. To qualify for a mortgage or license for a commercial enterprise, a building owner must carry fire insurance. Similarly, stakeholders may gain individually and collectively from the thriving cyber insurance markets in the future. Therefore, cyber insurance has the potential to be a significant risk management instrument for enhancing IT security. Theoretically, it provides resilience for both individual stakeholders and society as a whole [40].

2.7.2 CURRENT POLICIES AND MARKETS

Over the last five years, the market for cyber insurance has grown and become more distinct. However, few insurance companies include media/professional sale liability plans, though the majority now provide property, theft, and liability coverage [41]. Also, cyber insurance products are increasingly being created for niche industries; for instance, AIG and Chubb offer insurance for businesses that provide financial services. Moreover, prior to purchasing cyber insurance coverage, carriers and customers have to deal with security, making more sophisticated evaluations of safety. Depending on the risks to be covered and the desired policy limitations, carriers may demand audits by independent IT security consultants in a particular instance [42].

2.7.3 BARRIERS TO CYBER INSURANCE EXPANSION

Observers find the estimated acceptance rate of 25% for cyber insurance to be low. Especially in light of the well publicized rise in IT security incidents and increased

regulatory pressure to address them [42]. Several other aspects seem to have special importance for cyber insurance, which may partially explain how long it takes firms to recognize new security threats and budget for them. These issues have to do with asymmetric information, interrelated and insufficient reinsurance capability [43]–[48].

- **Asymmetric Information:** The asymmetric information problem, in which different parties have varying access to information, has been thoroughly studied by insurance industry. The results that hold for more mature insurance markets also hold for cyber insurance. However, asymmetric information affects insurance businesses both before and after the customer accepts an insurance contract. Insurers are faced with the adverse selection dilemma [21]–[27], wherein a customer who is more likely to suffer loss (due to hazardous behaviors or other possible innate variables) will find insurance for given rate more alluring than a customer who is less likely to do so. Also, the insurer won't be able to continue operating profitably if it can't distinguish between such customers and give differentiated premiums [15].
- **Interdependent and Correlated Risk:** Insurance companies must maintain a sizable policyholder base and insure risks that are largely unrelated and uncorrelated in order to deal with a regular stream of claims and prevent significant spikes in payouts. However, given the connected and interdependent risk in the context of cyber insurance, a majority of systems may be exposed to one incident if the installed systems have a monoculture [16]. For a variety of reasons, certain software market models tend to produce one dominant product. Also, given a monoculture of installed systems, such as the Microsoft Windows operating system [17], risk can also be interconnected. It means that one compromised system may affect risk to other systems. Worm assaults in particular, which make use of flaws in widely used software (often Microsoft Windows or Microsoft Outlook) spread from the infected systems and exhibit such traits [18].
- **Inadequate Reinsurance Capacity:** Large-scale natural catastrophes are types of incidents that cause numerous claims all at once in other insurance markets. By shifting some of their risk to adequately funded reinsurers in such circumstances, primary underwriters can still issue substantial individual policies and insure numerous parties who may be impacted by same incident, at the same time limiting their overall exposure. In essence, reinsurance is insurance that insurance firms buy. Reinsurance accounted for approximately half of the US\$83 billion in insured property damage. The projected global reinsurance capacity is US\$400 billion. In order to determine premiums and diversify risks geographically and to withstand even huge catastrophes like Katrina, reinsurers analyze loss data spanning several years [19].

2.8 REQUIREMENTS FOR CYBER SECURITY PROCESSES AND PROPOSED REGULATION

Three components make up proposed specifications. The needs for a cyber security management system (CSMS) in the automotive industry are discussed in the first

part, and the requirements for the post-production phase are covered in the next part. Approval of the vehicle type is covered in the last section. Also, the requirements for a cyber security management system and the requirements for vehicle types, as well as the CSMS Certificate of Compliance, are all included in the proposed regulation [49]–[53]. A list of the prerequisites is also provided [6].

2.8.1 CYBER SECURITY MANAGEMENT

The comprehensive framework that gathers all procedures important to cyber security is known as a cyber security management system, and car manufacturers must make sure that service providers and suppliers use a CSMS [54]. Also, an approval authority or technical service evaluates the CSMS of the manufacturer, suppliers, and service providers. Although technical service or approval authority may check the development, production, and post-production processes that are outlined in a CSMS at any time, the vehicle maker must notify the technical service or approval authority of any changes that might affect the evaluation and further must take into account the monitoring of risks and hazards to the vehicle as well as incident response procedures. The vehicle maker must distinguish between various life cycle definitions in the automotive area. According to UNECE regulations, a vehicle type's life cycle is defined as the period from development to start of production to the end of production. Therefore, lifetime is focused on the engineering of a system (element, component) that is to be used in numerous vehicles, according to ISO 26262 [55] and SAE J3061 [56], throughout the life cycle of production, use, and decommissioning for the actual vehicle. Also, the OEM must demonstrate that the company and every supplier involved have a certified CSMS in order to receive this type of clearance, for example, to begin manufacturing.

The following focus points should be included in the procedures to guarantee that security is appropriately taken into account:

- Organizational management of cyber security
- Risk management for the vehicle type (risk identification, evaluation, classification, and management)
- Verification of adequate risk management of those highlighted hazards
- Testing for security during development and production
- Cyber attack detection and reaction for various vehicle types
- Determining and managing emerging cyber risks and vehicle type vulnerabilities
- Updates to the risk analysis

2.8.2 POST-PRODUCTION PHASE

The post-production phase's requirements are primarily for the fine-tuning of the CSMS. Such criteria are to make sure that cyber security is included into the vehicle life cycle. Thus the maker of the vehicle must provide evidence of how protection and compliance with the law are upheld throughout the life of the vehicle. Further, it entails keeping track of modifications to the threat environment and vulnerabilities. Moreover, the effectiveness of implemented security measures has to be tracked, making sure that

evolving conditions don't have an impact on availability and safety. Thus processes for incident response must be in place in order to guarantee this safeguard [56]–[57].

2.8.3 VEHICLE TYPE

The OEM and suppliers have certified CSMSs in place. That enables a vehicle type approval to be completed. How the risk evaluation takes known vulnerabilities and threats into account must be included in the proof for the entire vehicle type approval. The entire vehicle, each vehicle system, and how they work together must be taken into account during the risk assessment [11]. Those important parts to be identified in the risk assessment are constructed and secured appropriately so that the risk is decreased to a manageable level. Elements consist of:

- Vehicle systems and architecture.
- Systems and components that is pertinent to cyber security.
- Interactions between cyber-security-related parts and systems and other internal and external systems in the vehicle to show that all risks are sufficiently mitigated; the chain from recognized risk to mitigation strategy applied to test outcome must be followed. It is necessary to have a specialized and secure environment. If vehicle supports the execution or storage of aftermarket software, services, or data, the necessary data must be gathered throughout the whole supply chain and confirmed [26].

2.9 STATE-OF-THE-ART OF AUTOMOTIVE CYBER SECURITY FRAMEWORK

A procedural structure for achieving cyber security over the whole life cycle of the vehicle is what UNECE demands. Thus every stakeholder with the ability to affect cyber security must be covered. By using this framework, the maker should be able to show why the vehicle's cyber security is successful, even though currently no comprehensive framework has been developed at the beginning. In the following sections, we will provide an overview of the:

1. Current cyber security procedures for the automobile industry.
2. Current assurance techniques.
During the process, we must choose between:
3. Methods for handling cyber security in pre-production, production, and post-production.
4. Processes addressing the automobile domain's scattered nature.
5. Risk management processes to be used to outline the first set of procedures, whereby the automotive supply chain management can be used to summarize the second set [39].

2.9.1 AUTOMOTIVE CYBER SECURITY RISK MANAGEMENT

In ISO 31000 [23], generic risk management processes are described. However, risk management is characterized as an iterative process that must be carried out

throughout the entire life cycle. NIST [24] provides the definition of risk management at the organizational and system levels. Both strategies broadly address the needs for a CSMS risk management.

- **Risk Identification:** Threat modeling is well-known technique for identifying automobile risks [25]. Threat modeling has been demonstrated to be useful for risk identifications due to design flaws and possible threats over the whole vehicle life cycle [26]. This can even be used to monitor deployed systems for vulnerabilities. Threat modeling can support the security testing process and can also be employed as a component of a combined methodology for safety and security [27]–[29]. According to recent methodologies, that has described work in the same way. Also, danger modeling depends on current information about the threat and cyber security landscape. This includes the monitoring of the broader threat landscape, as well as forensic capabilities for the vehicle.
- **Risk Assessment:** There are several approaches for risk assessment, some of which are also used in risk identification techniques. Also, standard criteria [30] that evaluate the attack probability serve to define a well established strategy. Depending on the information at hand and the stage of the life cycle, the attack likelihood can be adjusted, as the foundation for the EVITA project [31] as well as [32].
- The selection of risk identification and assessment techniques has been compiled [33] and published as part of the HEAVENS project. A unified quantitative risk assessment for safety and security based on FAIR was created as part of the CySiVuS project [34].
- **Risk Categorization:** The question of risk classification is still under debate. Current methods categorize risks as safety-relevant or not and propose classification under the headings of “Safety, Financial, Operational, and Privacy.” Other methods classify risks using automated methods [35].
- **Risk Treatment:** Risk management entails both the essential actions to confirm the efficacy of implemented measures as well as all feasible risk mitigation. Thus the automobile domain is a good place to start with defense-in-depth tactics [36]. Accordingly, technical risk management measures are typically separated into four tiers [37]:
 - **Interfaces:** A variety of modern vehicles’ interfaces could be employed as possible assault surfaces. The objective is to protect every interface while reducing the number of interfaces.
 - **Gateways:** Gateways are used to connect several bus systems, making them well suited to incorporate extra security measures in order to segregate network components and regulate access [38].
 - **Network Automotive Vehicles:** These use a variety of internal communication systems that are specifically designed for safety [39]. Cryptography solutions are limited in their application by performance. Also, intrusion detection systems are a good strategy because machine-to-machine communication is predefined [40].
 - **Control Units:** These assure device integrity. The majority of ways to secure control units use hardware-based security [41]. These techniques

can also be used to prevent tampering and to guarantee a secure boot. To guarantee that risk identification, assessment, and categorization are taken into account at the appropriate phases, risk treatment methods are performed in a secure manner, and processes for risk management need to be integrated into the life cycle process.

One of the first methods for safe development was SAE J3061, which was based on the process model specified by ISO 26262. The publication of ISO/SAE 21434 [42]–[43], a new standard for cyber security engineering for automotive systems, is planned for 2020. In addition to these standards, which primarily address the overall engineering process, IEC 62443 [44] and NIST publications like [45] are suitable for the production environment. Also, it is possible to integrate instructions for secure coding and instructions for using hardware-based security.

2.9.2 AUTOMOTIVE CYBER SECURITY SUPPLY CHAIN MANAGEMENT

The supply chain in this case covers both the aftermarket and tiered structure of the automotive sector [46] to guarantee the security of crucial information. For instance, an OEM can demand that its supplier provide information on the security of their systems [47]. By evaluating the environment using IEC 62443, the protected production environment may be proven. Also, process evaluations can also be done with the assistance of automotive SPICE [48]. Existing methodologies from safety can be applied for the assignment of duties and tasks. In the various stages of the vehicle life cycle, similar interface agreements can be utilized to specify roles. For instance, a company other than the car maker might be tasked with keeping an eye on the shifting danger and risk situation. With company like AUTO-ISAC, we witness the initial efforts in this direction [50]. Additionally, methods for disseminating incident information are crucial in this situation [51]. Examples of how various interface agreements could apply to various life cycle phases are shown in Figure 2.4.

Without a written agreement with the car manufacturer, managing an organization is more difficult. However, many of the Android Auto infotainment apps that are currently accessible have vulnerabilities, based on reverse engineering [52]. Another issue at hand is whether the car maker can ensure security by providing a secure execution environment if the system must also be regulated to only accept apps being evaluated by the car manufacturer. The diagnostic interface is potentially risky when a vehicle is being serviced, according to a related analysis [53]. The extended vehicle concept [54] is one suggestion to deal with issue. According to the extended vehicle concept, access to vehicle data is managed by a third party. Here is a potential conflict between security and controlled access rules. Thus, competition law restrictions present a challenge [55].



FIGURE 2.4 Examples of various interface agreements at various stages of the life cycle.

2.9.3 AUTOMOTIVE CYBER SECURITY ASSURANCE

Assurance is “grounds for justified confidence that claim has been or will be achieved,” according to ISO/IEC/IEEE 15025–1 [56]. Also, this is accomplished by using an assurance case, which consists of methodical reasoning, its supporting data, and its presumptions. ISO/IEC/IEEE 15025 provides a mathematical specification for the structure of an assurance case, yielding graphical notations like GSN [57]. Both strategies face the difficulty of having to take into account how cyber security is evolving, for example, how threat actors’ capabilities are growing. Also, the completeness and sufficiency of cyber security must be demonstrated by evidence. Completeness demonstrates that all risks are taken into account based on the state of the art, and sufficiency demonstrates that the way risks are handled is adequate by providing proof that a methodical approach was followed throughout the life cycle. Evidence for sufficiency must demonstrate that risks are adequately managed. The common criteria and testing recommendations from NIST [58] can be used to meet the assurance requirements for this. Its suggested methods begin with document reviews and include methods for ongoing testing. In the evaluation of systems that are already in use, determining when evidence is sufficient for cyber security assurance is one challenge [31].

2.9.4 CSMS FRAMEWORK

There is a need for a comprehensive framework that integrates development and operation and that covers the entire life span, as discussed in previous sections. Therefore, it is suggested that a DevOps strategy can be used to organize the development, production, and operation processes. The suggested framework is divided into two main sections and is based on earlier work by Dobaj et al. [29]–[30]. A fifth-generation vehicle E/E architecture first makes it possible to connect vehicle systems to cloud systems for ongoing monitoring and offers the technical basis for the construction of a modular system architecture. That is easily updated and reconfigurable [41].

A DevOps life cycle can be built up to create a continuous improvement cycle. On top of the modular E/E architecture. A key component of this life cycle is represented by the monitoring and analysis processes, the groundwork for identifying errors and security issues during both development and operation [34]. The suggested DevOps framework is compatible with conventional system development procedures, as shown by the V-Model. However, the same three primary steps make up both the development and the system improvement cycles: planning, implementation, and verification and validation (V&V). Improvement cycles are automatically initiated by monitor and analyze procedures, whenever a failure or security incident is recognized either in the V&V phase or during vehicle operation [37]. Information security management is used in the subsequent release phase to provide a mechanism for guaranteeing system integrity. During the distributed software deployment process, each vehicle independently ensures security in the succeeding prevent phase. Local analysis of anomalies is followed by transmission to an outside system [6].

2.10 CYBER SECURITY ISSUES AND CHALLENGES

Technology for information and communications (ICT) is pervasive. It is constantly changing with time and development in technology and plays an ever bigger role in contemporary society. ICT equipment and parts create a system of interconnected networks. Cyberspace is the name for the local data and infrastructure, and defending cyberspace against intrusions by thieves and other foes is known as cyber security. Thus, depending on three factors, such attacks pose hazards and vulnerabilities [32].

2.10.1 WHAT ARE THE THREATS?

Nation-state adversaries who develop capabilities and carry out cyber attacks in support of a country's strategic objectives are known as "hacktivists." These cyber attacks are carried out for nonmonetary reasons such as theft or extortion, and spies become involved in espionage and stealing proprietary information used by governmental or private entities [18].

2.10.2 WHAT IS A VULNERABILITY?

There is currently an arms race in cyber security between attackers and defenders. Attackers continuously look for flaws in ICT systems and for inadvertent or deliberate actions by system insiders with access to supply chain vulnerabilities that allow the insertion of malicious software [49].

2.10.3 WHAT IS AN IMPACT?

An impact affects the confidentiality, integrity, and availability of ICT system information and, depending on how it is connected could compromise everything with a successful assault. Financial, proprietary, and personal information may be infiltrated as a result of cyber theft or cyber espionage, which is carried out frequently without the victim's knowledge. However, attacks that cause a denial of service can impede or stop authorized users from using a system. Moreover, cyber attacks on systems and bonnet malware provide an attacker control of network of "zombie" computers. Attacks on industrial control systems can lead to the obliteration of the machinery, which might include centrifuges, pumps, and generators [7]–[15].

2.10.4 FEDERAL ROLE

The federal government's participation in cyber security includes both defending its own networks and aiding in the defense of non-governmental ones. Federal agencies also work for safeguarding their own systems, and many have CI obligations. Various areas of cyber security are covered by more than 50 pieces of legislation, and the 113th and 114th Congresses have passed a number of additional laws [41]–[43]. Generally speaking, NIST (National Institute of Standards and Technology) establishes FISMA (Federal Information Security Management Act of 2002) rules that apply to federal civilian ICT and OMB. These rules are intended to ensure

that they are put into practice. The Department of Homeland Security (DHS) is the principal agency coordinating government efforts to assist private firms in securing CI assets; their operational responsibility is to protect federal civilian networks. The DOJ is the primary enforcement body for the relevant legislation. The Department of Defense's (DOD) acts in cyberspace to ensure the safety of defense assets and civil authorities. These and the National Security System (NSS) are all under the purview of DOD. IC also includes the National Security Agency (NSA) [59].

2.10.5 LEGISLATIVE ACTIONS

More than 200 bills that deal with cyber security issues have been introduced since the 111th Congress in both the 113th and 114th Congresses. The legislation deals with a number of problems that include [60].

- **Federal Information Systems:** Giving DHS more authority to defend government networks and amending FISMA to reflect developments in the ICT environment [59, 61]
- **Information Sharing:** Allowing private sector organizations to monitor and manage defenses on their information systems and easing public and private sector sharing of information on cyber threats and defensive measures [59]
- **Program Authorization:** The National Science Foundation, NIST (framework for CI cyber security, education, and awareness), and DHS (the National Cyber-Security and Communications Integration Center [NCCIC] carried out their ongoing activities with specific statutory authorization [47].
- **R&D:** Updates to agency authorizations and strategic planning requirements [49]
- **Workforce:** Enforcing an employment code system for federal cyber security employees, thus increasing the size, expertise, and readiness of DHS cyber security workforce [41]

2.10.6 LONG-TERM CHALLENGES

The legislation and executive-branch initiatives mentioned are primarily intended to address cyber security needs. Also, it includes preventing cyber-based disasters, espionage, and minimizing the effects of successful attacks, as well as enhancing inter- and intra-sector collaboration and outlining the roles and responsibilities of federal agencies and combating cyber crime. But such requirements are there in the context of more challenging long-term issues with regard to design, incentives, consensus, and environment (DICE) [23]:

- **Design:** According to experts, ICT design must include effective security as a key component. Due to financial constraints, developers have typically given functionality a higher priority than security. Additionally, many future security requirements cannot be forecasted, which presents a challenging task for designers [59, 60], [62]–[65].

- **Incentives:** The economics for cyber security have been criticized for having a flawed or even distorted incentive structure. Also, cyber crime is thought to be relatively safe, profitable, and inexpensive for the offenders. In contrast, cyber security can be costly because it is inherently flawed and the financial returns on investments are frequently uncertain [44]–[58].
- **Consensus:** There is little shared understanding of what cyber security is, how it should be implemented, and the risks among the various stakeholders. Also, there are significant cultural barriers to consensus, not just within sectors but also among sectors [49]–[58], [66].
- **Environment:** In terms of size and characteristics, cyberspace has been dubbed the technological environment that is evolving quickly in human history. Emerging technologies such as social media, mobile computing, and the Internet of Things (IoT) just make the already challenging threat environment even worse. On certain issues, legislation and executive actions may have a big impact. For instance, cyber security research and development may influence the design of ICT. Also, cyber crime penalties may affect the design of incentives [62, 67].

2.11 CONCLUSION

Security is a compulsory part of any type of data. This research work respectively expounds on the problems of cyber insurance in security and the architecture of smart cities. Also, it focuses on cyber progress, regulation, issue, and automation in cyber security. Through this study, we draw attention to problems that still need to be remedied in order to increase SG security, privacy, and trust. In order to aid researchers in this emerging field, it is essential to introduce innovative ways to ensure the safety concern of future. Therefore, through optimal operation of SG, this can become reality. Moreover, future research directions from both the technological and the human perspectives were also presented.

REFERENCES

- [1] Abdul Jabbar, Rusul, et al. “Applications of artificial intelligence in transport: An overview.” *Sustainability* 11.1 (2019): 189.
- [2] Kumar, Gulshan, and Krishan Kumar. “The use of artificial-intelligence-based ensembles for intrusion detection: A review.” *Applied Computational Intelligence and Soft Computing* 2012 (2012).
- [3] Yildirim, Merve. “Artificial intelligence-based solutions for cyber security problems.” *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. IGI Global* (2021): 68–86.
- [4] Battina, Dhaya Sindhu. “Application research of artificial intelligence in electrical automation control.” *International Journal of Creative Research Thoughts (IJCRT), ISSN* (2015): 2320–2882.
- [5] Rich, E., and K. Knight. *Artificial Intelligence*, Second Edition, McGraw-Hill, 1991: 621.
- [6] You, Xiaohu, et al. “Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts.” *Science China Information Sciences* 64.1 (2021): 1–74.

- [7] Stallings, William. *Wireless Communications & Networks*, Second Edition, Pearson Education India, 2009.
- [8] Li, Xichun, et al. "The future of mobile wireless communication networks." *2009 International Conference on Communication Software and Networks*. IEEE, 2009.
- [9] García-Hernández, Carlos F., et al. "Wireless sensor networks and applications: A survey." *IJCSNS International Journal of Computer Science and Network Security* 7.3 (2007): 264–273.
- [10] Xu, Bangnan, Sven Hischke, and Bernhard Walke. "The role of ad hoc networking in future wireless communications." *International Conference on Communication Technology Proceedings, 2003. ICCT 2003*. Vol. 2. IEEE, 2003.
- [11] Wang, Meiyu, et al. "Transfer learning promotes 6G wireless communications: Recent advances and future challenges." *IEEE Transactions on Reliability* 70.2 (2021): 790–807.
- [12] Akyildiz, Ian F., Ahan Kak, and Shuai Nie. "6G and beyond: The future of wireless communications systems." *IEEE Access* 8 (2020): 133995–134030.
- [13] Groumpos, Peter P. "Artificial intelligence: Issues, challenges, opportunities and threats." *Conference on Creativity in Intelligent Technologies and Data Science*. Springer, 2019.
- [14] Ghallab, Malik. "Responsible AI: Requirements and challenges." *AI Perspectives* 1.1 (2019): 1–7.
- [15] Rodrigues, Rowena. "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities." *Journal of Responsible Technology* 4 (2020): 100005.
- [16] Borenstein, Jason, and Ayanna Howard. "Emerging challenges in AI and the need for AI ethics education." *AI and Ethics* 1.1 (2021): 61–65.
- [17] Khan, Inam Ullah, et al. "Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles." *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*. ACM, ST.PETERSBURG, RUSSIA, 2020.
- [18] Khan, Inam Ullah, et al. "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)." *IEEE Access* 8 (2020): 56371–56378.
- [19] Khan, Inam Ullah, et al. "Routing protocols & unmanned aerial vehicles autonomous localization in flying networks." *International Journal of Communication Systems* (2021): e4885.
- [20] Khan, Inam Ullah, et al. "Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing." *Journal of Healthcare Engineering* 2021 (2021).
- [21] Khan, Inam Ullah, et al. "Intelligent detection system enabled attack probability using Markov chain in aerial networks." *Wireless Communications and Mobile Computing* 2021 (2021).
- [22] Begum, Seema, et al. "Source routing for distributed big data-based cognitive internet of things (CIoT)." *Wireless Communications and Mobile Computing* 2021 (2021).
- [23] Sajid, Faiqa, et al. "Secure and efficient data storage operations by using intelligent classification technique and RSA algorithm in IoT-based cloud computing." *Scientific Programming* 2022 (2022).
- [24] Khan, Inam Ullah, et al. "A novel design of FANET routing protocol aided 5G communication using IoT." *Journal of Mobile Multimedia* (2022): 1333–1354.
- [25] Khan, Inam Ullah, et al. "Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS." *Computers, Materials and Continua* 70.2 (2022): 3653–3666.
- [26] Wang, Jun, et al. "Artificial intelligence and wireless communications." *Frontiers of Information Technology & Electronic Engineering* 21.10 (2020): 1413–1425.

- [27] Joung, Jingon. "Machine learning-based antenna selection in wireless communications." *IEEE Communications Letters* 20.11 (2016): 2241–2244.
- [28] Chen, Mingzhe, et al. "Wireless communications for collaborative federated learning." *IEEE Communications Magazine* 58.12 (2020): 48–54.
- [29] Verma, Abhishek, and Virender Ranga. "Machine learning based intrusion detection systems for IoT applications." *Wireless Personal Communications* 111.4 (2020): 2287–2310.
- [30] Jia, Guangyu, et al. "Channel assignment in uplink wireless communication using machine learning approach." *IEEE Communications Letters* 24.4 (2020): 787–791.
- [31] Gowdhaman, V., and R. Dhanapal. "An intrusion detection system for wireless sensor networks using deep neural network." *Soft Computing* 26.23 (2022): 13059–13067.
- [32] Chen, Mingzhe, et al. "Artificial neural networks-based machine learning for wireless networks: A tutorial." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3039–3071.
- [33] Jagannath, Anu, Jithin Jagannath, and Tommaso Melodia. "Redefining wireless communication for 6G: Signal processing meets deep learning with deep unfolding." *arXiv preprint arXiv:2004.10715* (2020).
- [34] Cai, Xiaoran, et al. "D2D-enabled data sharing for distributed machine learning at wireless network edge." *IEEE Wireless Communications Letters* 9.9 (2020): 1457–1461.
- [35] Lee, Hoon, et al. "Deep learning framework for wireless systems: Applications to optical wireless communications." *IEEE Communications Magazine* 57.3 (2019): 35–41.
- [36] Sharma, Pankaj. "Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network." *International Journal of Computer Science and Mobile Computing* 2.8 (2013): 47–53.
- [37] Vora, Lopa J. "Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G." *International Journal of Modern Trends in Engineering and Research* 2.10 (2015): 281–290.
- [38] Gawas, Anju Uttam. "An overview on evolution of mobile wireless communication networks: 1G-6G." *International Journal on Recent and Innovation Trends in Computing and Communication* 3.5 (2015): 3130–3133.
- [39] Yang, Ping, et al. "6G wireless communications: Vision and potential techniques." *IEEE Network* 33.4 (2019): 70–75.
- [40] Siriwardhana, Yushan, et al. "AI and 6G security: Opportunities and challenges." *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021.
- [41] Ahammed, Tareq Bin, and Ripon Patgiri. "6G and AI: The emergence of future forefront technology." *2020 Advanced Communication Technologies and Signal Processing (ACTS)*. IEEE, 2020.
- [42] Borah, Deva K., et al. "A review of communication-oriented optical wireless systems." *EURASIP Journal on Wireless Communications and Networking* 2012 (2012): 1–28.
- [43] Lee, Hoon, et al. "Deep learning framework for wireless systems: Applications to optical wireless communications." *IEEE Communications Magazine* 57.3 (2019): 35–41.
- [44] Lytvyn, Vasyl, et al. "Intelligent system of a smart house." *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*. IEEE, 2019.
- [45] Moslehi, Khosrow, and Ranjit Kumar. "A reliability perspective of the smart grid." *IEEE Transactions on Smart Grid* 1.1 (2010): 57–64.
- [46] Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." *IEEE Communications Surveys & Tutorials* 14.4 (2011): 944–980.
- [47] Al-Omari, Mohammad, et al. "An intelligent tree-based intrusion detection model for cyber security." *Journal of Network and Systems Management* 29 (2021): 1–18.

- [48] Azeez, Nureni Ayofe, et al. "Intrusion detection and prevention systems: An updated review." *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019* 1 (2020): 685–696.
- [49] Kruegel, Christopher, and Thomas Toth. "Using decision trees to improve signature-based intrusion detection." *Recent Advances in Intrusion Detection: 6th International Symposium, RAID 2003, Pittsburgh, PA, USA, September 8–10, 2003. Proceedings* 6. Springer, 2003.
- [50] Jyothsna, V. V. R. P. V., Rama Prasad, and K. Munivara Prasad. "A review of anomaly based intrusion detection systems." *International Journal of Computer Applications* 28.7 (2011): 26–35.
- [51] Alshehri, Fatima, and Ghulam Muhammad. "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare." *IEEE Access* 9 (2020): 3660–3678.
- [52] Chen, Xieling, et al. "Information fusion and artificial intelligence for smart healthcare: A bibliometric study." *Information Processing & Management* 60.1 (2023): 103113.
- [53] Ragavi, B., et al. "Smart agriculture with AI sensor by using Agrobot." *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2020.
- [54] Qazi, Sameer, Bilal A. Khawaja, and Qazi U. Farooq. "IoT-equipped and AI-enabled next generation smart agriculture: A critical review, current challenges and future trends." *IEEE Access* 10 (2022): 21219–21235.[55] Choo, Kim-Kwang Raymond. "The cyber threat landscape: Challenges and future research directions." *Computers & Security* 30.8 (2011): 719–731.
- [56] Stevens, Tim. "Knowledge in the grey zone: AI and cybersecurity." *Digital War* 1 (2020): 164–170.
- [57] Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." *Cyber, Intelligence, and Security* 1.1 (2017): 103–119.
- [58] Repalle, Syam Akhil, and Venkata Ratnam Kolluru. "Intrusion detection system using ai and machine learning algorithm." *International Research Journal of Engineering and Technology (IRJET)* 4.12 (2017): 1709–1715.
- [59] Shahzad, Abdul Qahar, and Mona Lisa. "UAV-based photogrammetry and seismic zonation approach for earthquakes hazard analysis of Pakistan." In *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*. Cham: Springer International Publishing, 2022: 211–224.
- [60] Shahzad, Abdul Qahar, Mona Lisa, Mumtaz Ali Khan, and Irum Khan. "UAV-based rescue system and seismic zonation for hazard analysis and disaster management." In *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*. Cham: Springer International Publishing, 2022: 245–262.
- [61] Baig, Bisma, and Abdul Qahar Shahzad. "Machine learning and AI approach to improve UAV communication and networking." In *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*. Cham: Springer International Publishing, 2022: 1–15.
- [62] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: Classification and state-of-the-art." *Computer Networks* 44.5 (2004): 643–666.
- [63] Bassil, Ramzi, et al. "Security analysis and solution for thwarting cache poisoning attacks in the domain name system." *2012 19th International Conference on Telecommunications (ICT)*. IEEE, 2012.
- [64] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. "A survey of solutions to the sybil attack." Technical Report of University of Massachusetts Amherst, Amherst, MA 7 (2006): 224.

- [65] Yihunie, Fekadu, Eman Abdelfattah, and Ammar Odeh. "Analysis of ping of death DoS and DDoS attacks." *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2018.
- [66] Modi, Chirag, et al. "A survey of intrusion detection techniques in cloud." *Journal of Network and Computer Applications* 36.1 (2013): 42–57.
- [67] Chao-Yang, Zhang. "DOS attack analysis and study of new measures to prevent." *2011 International Conference on Intelligence Science and Information Engineering*. IEEE, 2011.

3 Comparative Analysis of Machine and Deep Learning for Cyber Security

*Hafsa Maryam, Syeda Zillay Nain
Zukhruf, and Rehmat Ullah*

3.1 INTRODUCTION

In today's world, networks are becoming increasingly influential, widespread, and interconnected, making cyber security a critical area of research and development. It is necessary to protect networks, devices, and the data against any kind of unauthorized access, theft, and damage. However, new technologies like smart devices, cloud computing, the Internet of Things (IoT), and big data make it increasingly challenging to protect data from various types of threats, including cyber attacks [1]. Intelligent techniques are needed to detect these malicious attacks. Many different techniques are used to build a robust security system. Recently, fundamental data security learning methods have made significant progress in detecting attacks such as intrusion detection systems (IDS) [2]. These systems help to identify and monitor various types of attacks on network traffic activity, making IDS an essential tool in detecting cyber attacks and network intrusions. Cyber security plays a vital role in protecting networks and data by detecting various cyber attacks and network intrusions.

The frequency of miscellaneous cyber attacks has increased significantly in recent years. Normally, there exist two types of attacks: active and passive [3, 4].

The impact of a cyber attack can range from mild inconvenience to severe financial losses and reputational damage. There are several types of cyber attacks, including phishing attacks, man-in-the-middle attacks, and malware attacks [5, 6]. Malware attacks involve the installation of malicious software on a victim's device to damage or gain unauthorized access to their system. A man-in-the-middle attack happens when an attacker intercepts the communication between two groups and can lead to information theft or unauthorized access [7].

To detect and prevent cyber attacks, organizations and individuals use different techniques. One approach uses intrusion detection systems (IDS) that are designed to keep a check on network traffic and identify any potential threats. IDS can detect abnormal behavior, such as unauthorized access attempts or suspicious network activity, and alert security teams for further investigation. Another approach is using

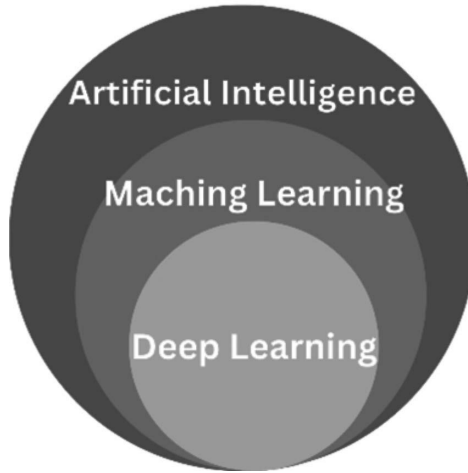


FIGURE 3.1 Overview of AI architecture.

phishing detection systems, designed to identify and block suspicious emails and links. Malware detection systems work in a similar way by scanning files and email attachments for known malware signatures and behaviors. Man-in-the-middle attack detection systems monitor network traffic for signs of interception or unauthorized access. These systems can detect and alert security teams to potential threats in real time allowing for immediate response and mitigation [8, 9].

Researchers are currently exploring how cyber detection techniques, such as intrusion detection systems (IDS), can contribute to achieving a type of collective intelligence as shown in Figure 3.1. By applying different technologies like intelligent systems, agents, and other techniques, networks can be secured more accurately, improving the performance in detecting threats and attacks [10]. ML and DL classifiers provide solutions for cyber attacks [11].

ML and DL techniques have proven to be powerful tools in various fields, and they can be integrated with cyber security systems to enhance an organization's security measures. Several ML and DL applications are used to protect businesses and products from malware and hacker attacks. To ensure effective denial of service (DoS) attacks and malware analysis, efficient strategies are required because cyber crime remains a growing concern with respect to protection and privacy [12, 13].

This research provides a brief study about ML and DL techniques for cyber security. Also, this chapter covers the publication trend of past decades as well as future trends of publication in the coming five years. Furthermore, this chapter covers the eye-opening future challenges in cyber security.

3.2 AI FOR CYBER SECURITY

As the development of cyber security systems has progressed, researchers have started to explore the use of techniques by AI [14]. AI's role in cyber security is expanding every day, which is used to secure overall network. AI, GA, and PSO are used to solve

related problems of cyber security [15]. The use of AI in cyber security has provided a remarkable and extraordinary capability to detect and prevent cyber attacks, leading to cutting-edge and transformative improvements in cyber security systems [16].

3.3 ML FOR CYBER SECURITY

ML is the subcategory of AI. It is closely related to computational statistics and has strong ties to mathematical optimization to design models and deliver various applications [17]. Arthur Samuel et al. initially provided the idea about ML where computers need to be able to learn like humans [18]. ML has become a powerful tool in the fight against cyber crime, with both attackers and defenders using the latest techniques to gain an advantage. Cyber criminals are constantly developing new ways to exploit weaknesses in computer systems, and ML can help them identify these vulnerabilities quickly and efficiently. On the other side of the fence, ML models are being used to create sophisticated defense mechanisms that can detect attacks in their early stages, minimizing the damage they cause. By combining different ML techniques, cyber defense systems can accurately identify and classify attacks, improving their overall effectiveness in safeguarding computer networks and systems.

- *Supervised learning* is one of the types of ML and aims to understand the relationship between input and output data. Once this relationship is established, the algorithm can predict the output for new input data based on what it has learned and mainly focuses on classification and regression methods. **Classification** groups similarly breaks down data points into different classes. This supervised approach finds the best way to separate the data points and assign them to specific classes. On the other side, **regression** differs from classification in that it outputs a number instead of assigning data points to classes. Classification focuses on classifying and outputting the class, whereas regression produces a numerical output [19].
- In *unsupervised learning*, the given dataset only has input data, and it deals with unlabeled data. Its purpose is to identify patterns or similarities in the dataset. After obtaining the features, it then groups the data based on those similarities [19]. Unlike supervised learning, the training process is unique since the algorithm learns from its own experiences instead of a predetermined set of inputs with an established relationship. In the absence of training data, the algorithm must rely on its own experiences to learn.

ML has revolutionized the field of cyber security and is continuously evolving to provide better and more efficient ways to combat cyber threats [20]. ML-aided types are used for detecting and preventing cyber attacks. *Supervised learning* techniques are used for detecting known threats and classifying new threats into categories such as malware, phishing, and spam. *Unsupervised learning* techniques, on the other hand, are used for identifying unknown threats and anomalies that are not part of the known threat categories. With the increasing number and complexity of cyber threats, these machine learning types are particularly useful for cyber detection because they can identify patterns and anomalies that might not be immediately

apparent to human analysts and that might be becoming more crucial in securing computer networks and systems [21].

3.3.1 ML TECHNIQUES APPLIED FOR CYBER DETECTION/CYBER SECURITY

In the realm of cyber detection, cyber attackers, and cyber security defenders, cyber criminals are utilizing ML techniques to identify vulnerabilities in systems and to develop advanced attack methods that can penetrate defense mechanisms. ML models are used to improve military applications, especially attack detection systems. Therefore, due to early threat detection, better decisions will be made to reduce the impact of cyber attack [22, 23]. By the previously mentioned techniques, cyber attacks can be easily monitored [24]. A comprehensive list of these ML techniques is presented in Table 3.1 and discussed in Section 3.5. These techniques have been surveyed for cyber detection in Section 3.6, and a comparative analysis has been performed in Section 3.7.

In the cyber detection field, various ML techniques have been explored in the literature. This section focuses on the most commonly applied techniques. In *supervised-learning*, ML techniques can be further categorized into classification and regression [25]. In *unsupervised learning*, clustering (K-means) algorithm, and dimensionality reduction (PCA) are widely used techniques [26–27] and discussed in Section 5.

3.4 DL FOR CYBER SECURITY

DL is a subfield of ML, and it is a powerful ML approach that includes multiple neural networks with input, hidden, and output layers, which utilizes algorithms that are inspired by the human brain for analytical and logical thinking [28–29]. These areas have garnered significant attention from the academic community and research in the last decade [30–33]. DL is well-suited for handling large datasets and can effectively overcome the overfitting problem by creating generalized models.

DL plays a critical role in cyber detection and prevention. Its capability to process and analyze vast amounts of complex data quickly and accurately makes it a valuable tool for detecting and predicting cyber threats [30]. Additionally, DL can be used to analyze large volumes of security data to identify new threats and vulnerabilities. On the other side of the coin, cyber attackers are also leveraging DL to develop more complex and targeted attacks. DL is becoming an increasingly important aspect of cyber security and it can be used to optimize security policies and responses to cyber attacks, allowing for more efficient and effective cyber threat prevention and detection [30].

DL models are mainly focused on variable availability.

- *Supervised learning* is goal driven and relies on a defined target variable.
- *Unsupervised learning* is data-driven and the outcome is based solely on the input.

DL types are being used in several studies to improve cyber security [34–36]. DL supervised and unsupervised learning are both important for cyber security.

Supervised learning can be used for detecting known threats and classifying new threats into categories such as malware, phishing, and spam. As cyber threats continue to evolve and become more complex, this type of learning is task driven and has well-defined goals, making it useful for cyber attack prevention and detection. On the flip side of the coin, *unsupervised learning* can be used for identifying unknown threats and anomalies that are not part of the known threat categories. This type of learning is crucial for the early detection of novel cyber threats and cyber attack prevention [37].

3.4.1 DL TECHNIQUES APPLIED FOR CYBER DETECTION/CYBER SECURITY

DL techniques can be trained to recognize patterns and anomalies in large datasets, enabling accurate and prompt detection of cyber attacks. Cyber attackers use DL techniques to develop sophisticated attacks that can bypass traditional security systems. For example, attackers may use deep learning to generate realistic phishing emails that are designed to deceive users into providing sensitive information or to create malware that can evade traditional antivirus software. On the other hand, cyber security defenders are also using DL techniques to detect and prevent cyber attacks. For example, DL can be utilized to analyze network traffic to detect suspicious activity or to scan for malware in real time. Also, it is being applied in the field of cyber detection to enhance the accuracy of detection and classification of cyber threats. Overall, DL techniques are playing an increasingly important role in both cyber attacks and cyber security. As the field of AI continues to advance, it is likely that DL will become even more important in the fight against cyber crime. Moreover, the DL technique employs an *unsupervised* layer-by-layer greedy training algorithm that offers promising solutions for optimizing deep structures in cyber detection [38, 39]. Table 3.2 presents a comprehensive list of DL techniques that have been surveyed for cyber security in Section 3.8 and a comparative analysis of these techniques has been conducted in Section 3.9.

In the cyber security domain, a plethora of studies have been available on DL techniques, and they can be further categorized into supervised and unsupervised learning:

- In *supervised*, there are various techniques including fully connected feed-forward deep neural network, recurrent neural network (RNN), which is further categorized into long short-term memory (LSTM), bidirectional-RNN (Bi-RNN), and GRU, multilayer perceptron free forward deep neural network, and convolutional deep neural network (CNN).
- In *unsupervised*, GAN, RBM, autoencoders, further categorized into stacked autoencoders, are involved and discussed in Section 3.5 and Table 3.1.

3.5 ML AND DL TECHNIQUES

In this section, both ML techniques are discussed and DL techniques are discussed in detail. ML and DL techniques can be overviewed in Table 3.1 and 3.2 as well as illustrated in Figure 3.2.

TABLE 3.1
OVERVIEW OF ML TECHNIQUES

	ML-Model	Year	Description	Limitations	Ref.
Supervised	Naïve Bayes	1960s	A probabilistic algorithm that assumes the independence of features given the class label to predict the class of new data points and take less computational time Particularly suited for high-dimensional datasets with discrete features	Assumes independence of features, can be sensitive to irrelevant features, may suffer from the “zero frequency” problem	[40–42]
	<i>K</i> -nearest neighbor (<i>K</i> -NN)	1967	Lazy learning algorithm that classifies new data points by finding the <i>k</i> -nearest neighbors in the training set and assigning the majority class. The distance between data points can be measured using various distance metrics.	Case-sensitive to noisy data packets, choice of distance-metric and value of <i>k</i> can usually affect its performance. Computationally expensive when the dataset is large and may require the storage of the entire training set	[43, 44]
	SVM	1995	SVM separates and classifies data points based on their position relative to a hyperplane. Maximizing the margin and distances between hyperplanes increases classification accuracy SVM can be linear or nonlinear.	Processing a lot of memory is required as well as time for training Training is important for optimal results. Kernel-function and metrics used to have direct effect on performance of classifier	[45, 46]
	Decision tree	1986	Supervised ML technique based on a recursive tree structure Each tree is used to have parent node DT is based on IG and entropy.	DT can easily overfit the training data, leading to poor generalization performance. Sensitive to the small perturbations in the data, which can lead to the different tree structure.	[47–48]
	Random forest	1995	Ensemble learning algorithm that combines multiple decision tree	Difficulty in selecting decision trees during prediction.	[49, 50]

Unsupervised	<i>K</i> -means clustering	1995	Partitions data into k clusters by iteratively assigning data points to the nearest cluster center and updating the cluster centers. Process is repeated until convergence. Distance between data points is measured using the Euclidean distance metric.	Distance maybe sensitive to the initial choice of cluster centers and may converge to a suboptimal solution. Choice of k also requires some prior knowledge or experimentation. Computationally expensive when the dataset is large or the number of clusters is high	[51]
	PCA	1901	Reduces the number of dimensions in a dataset while preserving the most important information Linear method that calculates a new set of orthogonal variables that maximize the variance in the data Number of components is chosen based on the amount of variance they explain.	Preserves all the important information in the data and may lead to a loss of interpretability Nonlinear methods may be necessary for more complex datasets. The choice of the number of components requires some experimentation. Computationally expensive, especially for large datasets with many features	[52]

TABLE 3.2
OVERVIEW OF DL TECHNIQUES

	ML Model	Year	Description	Limitations	Ref.
Supervised	RNN	1982	Sequential data is used. RNNs use recurrent connections to store and pass information from previous time steps.	RNNs can suffer from the vanishing gradient problem, where the gradients used to update the weights in the network become very small, making learning difficult. Particularly pronounced for long sequences. Additionally, RNNs have difficulty learning long-term dependencies in the data.	[53, 54]
	LSTM	1997	LSTMs are particularly good at learning long-term dependencies in sequential data.	Sensitive LSTMs can still suffer from the vanishing gradient problem, although to a lesser extent than regular RNNs. LSTMs have a large number of parameters, which can make them difficult to train and prone to overfitting.	[55]
	CNN	1988	A type of neural network designed to work with grid-like data, such as images. CNNs use convolutional layers to extract features from the input data, which are then used to make predictions.	CNNs can struggle with handling sequential or time series data, since they are designed to work with grid-like data. CNNs use to have overfitting problem.	[56–61]
	DBN	2006	A type of neural network designed to learn a hierarchical representation of the input data. Use multiple layers of hidden units, with each layer learning to represent increasingly abstract features of the input data.	Difficult to train due to the large number of parameters involved. DBNs can struggle with handling sequential data, since they are designed to learn a hierarchical representation of the input data rather than explicitly modeling dependencies between adjacent time steps.	[62, 63]

Unsupervised	GAN	2014	The two parts are generator and a discriminator, trained together in a game-like setting.	GANs can be difficult to train, since the generator and discriminator need to be trained together in a game-like setting. GANs can suffer from mode collapse, where the generator learns to only generate a limited set of samples rather than a diverse set.	[64]
	RBM	2006	RBMs connected to every unit in the other layer.	RBMs can be difficult to train, since they require a lot of computational resources to learn the probability distribution over the input data. RBMs can struggle with handling sequential data, since they are designed to learn a probability distribution over the input data rather than explicitly modeling dependencies between adjacent time steps.	[65]
	Autoencoders	1987	Reduces a type of neural network that learns to encode and decode the input data. Autoencoders use an encoder to compress the input data into a lower-dimensional representation and a decoder to reconstruct the input data from the compressed representation.	Autoencoders can suffer from overfitting.	[66]

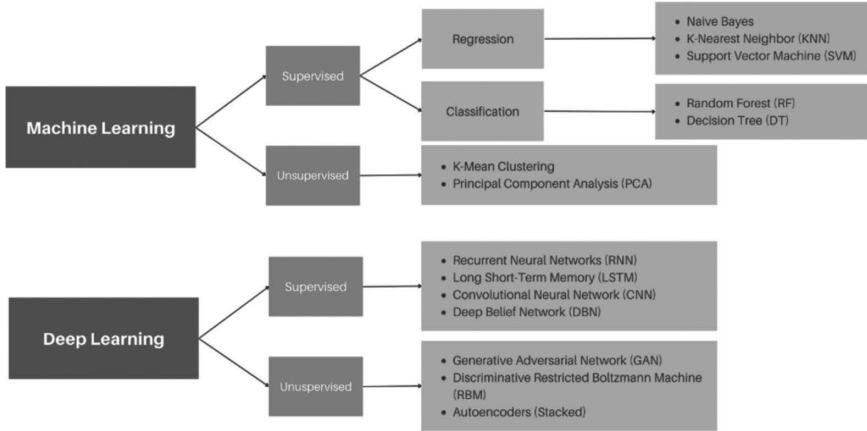


FIGURE 3.2 Overview of ML and DL techniques.

3.5.1 NAÏVE BAYES (NB)

NB is a method to predict high levels of probability as predicted. However, multi-feature-based datasets are dependent on one another, and there is an issue with different attack types. An improved version was introduced, called HiddenNB, that can handle mentioned issues and increase the level of accuracy up to 99.60%. Furtherly, the NB technique is efficient in the calculation of discrete categories. In addition, the NB model consists of three different techniques: Bernoulli, Gaussian, and multinomial. The multinomial NB technique is suitable for discrete categories, Bernoulli naïve Bayes for binary feature vectors and Gaussian naïve Bayes for continuous values of data [40–42]

3.5.2 K-NEAREST NEIGHBOR

The K-nearest neighbor (*K*-NN) is an algorithm used for unsupervised learning, and it relies on a distance function to evaluate the dissimilarity between two data instances. Compared to other classifiers, *K*-NN requires less time for training. The assumption underlying *K*-NN is that similar data points will be closer to each other in space, while dissimilar ones will be farther away. *K*-NN used to have two different categories that can be utilized for anomaly identification. The *K*th neighbor data point and density of each data instance are used to calculate scores [43]. The selection of the *k*th data point has a high effect on the classifier’s overall performance. *K*-NN is quite helpful in data analysis, which easily estimates distance function between data points. Moreover, this technique is computationally expensive because it needs a high level of storage capacity. The most common way to calculate the difference between two data points is by using Euclidean distance $d(m, n)$ [44].

3.5.3 SUPPORT VECTOR MACHINE (SVM)

SVM mainly relies on hyperplane approach. However, maximizing margin and distances between hyperplanes can improve results. SVM use to have two main

categories which include linear and nonlinear. While, single/multiclass are based on kernel function [45–46].

3.5.4 DECISION TREE (DT)

A decision tree is a data structure used to represent a series of decisions and their possible outcomes. The decision tree is an efficient technique to provide possible solutions for classification-based issues. However, the leaf node presents the final output. The DT technique is mainly based on entropy and information gain. Various techniques like ID3, C4.5, and CART can be utilized for designing the decision tree. ID3 is considered a classic greedy method used to select the optimal attribute. The splitting technique is found in C4.5, which is the expansion of ID3. However, CART is used to support both classification and regression. The C4.5 demonstration is available on the Weka tool [47, 48].

It is worth noting that DT has its limitations. For instance, it can create complex trees that are difficult to interpret, which can cause overfitting or underfitting. Also, the decision tree is sensitive to the data's distribution and can create biased trees that affect the classifier's accuracy.

The development of DT started in the late 1950s, and, since then, different versions and algorithms have been developed to improve its performance. ID3 was developed in 1986, C4.5 in 1993, and CART in 1984. These algorithms are widely used and have been implemented in various software and programming languages.

3.5.5 RANDOM FOREST (RF)

Random forest (RF) is an ensemble learning algorithm that combines multiple decision trees to produce a hypothesis for a problem, making it suitable for regression and classification tasks. RF is the new extension of CART, which is based on a multiple decision tree approach. However, RF applications are quite diverse and include malicious, abnormal, and illegal data packets detection. The previously mentioned RF technique uses less time and is less complex in the training module [49, 50]. However, consideration of decision trees during the prediction process can be a challenge.

3.5.6 K-MEANS CLUSTERING

This technique is used for clustering to calculate mean value. This process is repeated again and again to stabilize the overall network. *K*-means has applications in intrusion detection, spam filtering, and image segmentation [51].

3.5.7 PRINCIPAL COMPONENT ANALYSIS (PCA)

PCA seeks to find a set of orthogonal (uncorrelated) axes, or “principal components,” that explain the largest amount of variance in the data. The first principal component is the direction with the highest variance, the second principal component is the direction with the second highest variance, and so on. Once these principal components are identified, the data can be projected onto a lower-dimensional

subspace by selecting a subset of the principal components that account for a desired amount of variance [52].

3.5.8 RECURRENT NEURAL NETWORK

A recurrent neural network (RNN) is a type of neural network that utilizes hidden states. RNN is particularly useful in processing time series data and in analyzing data streams as it possesses memory and can retain information from previous experiences [53, 54].

3.5.9 LONG SHORT-TERM MEMORY (LSTM)

LSTM is quite helpful in IDS for attack detection. A special memory cell is stored over a long period of time in LSTM. LSTM is widely used in natural language processing (NLP) tasks, such as machine translation, speech recognition, and text classification [55].

3.5.10 CONVOLUTIONAL NEURAL NETWORK (CNN)

CNN use to have multilayer neural network, which is the new version of feed-forward-ANN [56]. However, CNN has three main layers: convolutional, connected, and pooling. Common CNN architectures include ZFNet [57], GoogLeNet [58], and ResNet [59]. CNN is widely used in many fields of study [60, 61]. Improved versions of CNN have also been proposed for intrusion detection and malicious traffic classification.

3.5.11 DEEP BELIEF NETWORK (DBN)

DBN is based on a greedy approach. It is designed to simulate and to process as a human brain processes complex information and recognize complex patterns. This technique can be used as a stack having generative nature [62, 63].

3.5.12 GENERATIVE ADVERSARIAL NETWORK (GAN)

GAN is considered subcategory of deep neural network that is used for generative modeling. GAN consists of two networks: a generator network and a discriminator network. The generator network generates new data samples that are similar to the training data, while the discriminator network tries to distinguish between the generated samples and the real ones. The two networks are trained together in a mini-max game, where the generator tries to fool the discriminator, and the discriminator tries to correctly identify the generated samples. GAN is used in a variety of applications, such as image synthesis, text-to-image generation, and video prediction [64].

3.5.13 RESTRICTED BOLTZMANN MACHINES (RBM)

Restricted Boltzmann machines (RBM) are a type of generative artificial neural network that follow an unsupervised learning approach. RBM consists of two layers of

nodes—visible layer and hidden layer—and each layer has a set of neurons. RBM tries to learn the distribution of the input data by updating the weights linking the nodes of the visible and hidden layers. The weights are updated using a technique called contrastive divergence [65]. RBM is used for a wide range of applications, such as image recognition, speech recognition, and collaborative filtering.

3.5.14 AUTOENCODER

Autoencoder is an unsupervised neural network used to reduce noise. Autoencoder consists of four parts: encoder, bottleneck, decoder, and reconstruction loss. The encoder learns how to compress the data. [66].

3.6 COMMONLY USED CYBER SECURITY DATASETS

ML techniques are quite helpful in detecting cyber threats. However, simulating a novel dataset is considered a tough job. A benchmark dataset can be used by many researchers, providing convenience and reliability. Using already available network security datasets can save a lot of time and increase the research efficiency by providing quick access to the required data for research.

3.6.1 DARPA IDS DATASET

The DARPA Intrusion Detection Data Sets, under the direction of DARPA and AFRL/SNHS, are collected and published by The Cyber Systems and Technology Group of MIT Lincoln Laboratory for evaluating computer network IDS [67]. This standard dataset provides a large amount of background traffic data and attack data, with three primary data subsets: (1) the 1998 DARPA Intrusion Detection Assessment Dataset, which includes seven weeks of training data and two weeks of test data; (2) the 1999 DARPA Intrusion Detection Assessment Dataset, which includes three weeks of training data and two weeks of test data; (3): the 2000 DARPA Intrusion Detection Scenario-Specific Dataset, which includes LLDOS 1.0 Attack Scenario Data, LLDOS 2.0.2 Attack Scenario Data, and Windows NT Attack Data [68].

3.6.2 KDD CUP 99 DATASET

The KDD Cup 99 dataset is a widely used training set for IDS, based on the DARPA 1998 dataset. It contains 4.9 million replicated data points containing total of 22 types of attack [69]. KDD Cup 99 is used to provide a full set of training and testing datasets. The so-called 10% subset was created to address the huge amount of connection records present in the full set, with some DoS attacks having millions of records [70]. Training and testing datasets have different probability distributions, and the 10% subset was intended for training while the corrected subset can be used for performance testing with over 300,000 records containing 37 different attacks. Moreover, the testing set has specific attack types that do not appear in the training set, making it a more realistic basis for IDS [71, 72].

Finally, the KDD data is old and no longer accurately represents the current network environment [73, 74].

3.6.3 NSL-KDD DATASET

This dataset is considered the new version of the previous one. This dataset contains 22 different attack types, which are categorized into four major groups. It is comprised of the KDDTrain+ dataset as the training set and the KDDTest+ and KDDTest-21 datasets as the testing set [75]. The latter is more challenging to classify due to its unbalanced representation of normal and attack records. However, the NSL-KDD still lacks up-to-date data, particularly for minority class samples. Despite this limitation, the dataset represents a significant improvement over its predecessor and serves as a valuable resource for network intrusion detection research.

3.6.4 ADFA DATASET

The ADFA dataset specifically consists of datasets for host-level intrusion detection systems and is commonly utilized in cyber science [76]. Kernel is considered the main facility to interact between the user space and kernel space. ADFA-LD is presented in figure. Further, data can be found on two different platforms, which include Linux and Windows.

3.6.5 UNSW-NB15 DATASET

The UNSW-NB15 dataset was formulated by the University of South Wales. The field of IDS relies on a variety of datasets, including UNSW-NB15, CAIDA, ADFA-LD, and UNM [77, 78]. As a new and representative IDS dataset, the UNSW-NB15 has been utilized and currently has less influence than the KDD99 [79].

3.7 SURVEY OF ML-AIDED TECHNIQUES IN CYBER SECURITY

This section presents different machine-learning-aided techniques proposed for cyber attack detection, which have been evaluated on different datasets with performance metrics. The proposed methods include both supervised and unsupervised techniques and various ML-aided techniques proposed for cyber attack detection, evaluated on different datasets with performance metrics.

In the supervised techniques, five different methods have been proposed for detecting different types of attacks. In [80], a naïve Bayes classifier to accurately classify the labeled data into the attack and normal classes. The results show improved accuracy, precision, and recall. In [81], clustering is used to extract cluster centers and identify the nearest node. The K -NN and K -means algorithms are used for this method, and the results show improved recall and accuracy.

In [82], the proposed method uses a one-class SVM to evaluate the practical feasibility of incorporating contextual and quantitative information of net flow records using a specific kernel function. The results show high accuracy. In [83], three experiments were conducted to evaluate RT-IDS for different machine-learning

classification approaches. The results show that the DT algorithm achieves the highest accuracy, while the NB algorithm has the lowest. In [84], the proposed IDS is implemented with a neuro tree for improved detection accuracy. The results show improved accuracy for both the RF and the C4.5 algorithms.

In the unsupervised techniques, two different methods have been proposed. In [85], a new method was proposed that combines many different techniques. The results show improved precision and recall. In [86], a new dataset is created by combining the voted outputs of built models on the GA suggested features of the NSL KDD dataset based on five different labels, followed by executing kernel extreme learning machine (KELM) with optimized parameters using GA. The results show high accuracy, recall, and precision for SVM, MLP, DT, and *K*-NN algorithms (Table 3.3).

3.8 SURVEY OF DL-AIDED TECHNIQUES IN CYBER SECURITY

In [87], a supervised approach is described that uses the RNN technique for cyber threats. Other research [88] uses another supervised approach that uses long short-term memory (LSTM) to secure channels. In [89], a supervised approach is simulated to identify specific categories of images in emails, achieving an accuracy of 75.10%. Another supervised approach [90] compares two deep neural network architectures, deep belief networks (DBNs), and cortical algorithm (CA) DNNs, for email spam classification on the Spam base dataset. The CA DNN architecture achieved higher accuracy than DBN with a six-layer architecture and decreasing hidden neurons, achieving an accuracy of 96.40%.

Researchers [91] have also described an unsupervised approach that uses deep learning-based anomaly detection methods, including de-noising autoencoder (DAE), stacked autoencoder (SAE), generative adversarial network (GAN), and DBM-Bi LSTM-based classification model, for detecting web attacks on the CSIC2010v2 dataset, achieving a precision, recall, and F1-score of 98.78%, as well as an accuracy of 98%. Another unsupervised approach [92] is used for cyber threat detection using KDD-99-dataset. The method achieved simulation results of around 94% when trained and tested on real data and 84–85% when trained on the KDD dataset and tested on real data. However, [93] describes an unsupervised approach to detecting false-data-injection attacks on smart grid. The experiments were conducted on generated data from the IEEE 14-bus, IEEE 30-bus, and IEEE 57-bus systems and the MATPOWER library. Table 3.4 provides information on different intrusion detection methods for various attack types, including supervised, unsupervised approaches, and datasets.

3.9 COMPARATIVE ANALYSIS OF ML/DL IN CYBER SECURITY

In this section, the comparative analysis of ML and DL in cyber security suggests that DL techniques have the potential to outperform traditional ML techniques in complex and large-scale datasets. However, the reliability and interpretability of DL models remain a challenge, making ML techniques still a popular choice for cyber security applications.

TABLE 3.3
SURVEY OF ML-AIDED TECHNIQUES

	Ref	Attack Type	Proposed Solution	ML-Aided Technique	Dataset	Performance Evaluation Matrix	Result
Supervised	[80]	Attack, normal	The proposed KMC + NBC algorithm comprises two main modules, preclassification and classification. The preclassification module utilizes the labels accordingly. The second module employs the naïve Bayes classifier to accurately classify the labeled data into attack and normal classes, resulting in improved detection accuracy.	NB, <i>K</i> -means	ISCX	NB Precision: 85.07% NB Recall: 99.70%	Accuracy of NB:88.28% Accuracy of <i>K</i> -means: 99.03%
	[81]	DoS, R2L, U2R, Probe	The proposed method involves clustering to extract cluster centers and identify the nearest neighbor of each data point in the same cluster based on the number of classes to be classified. In the second step, the distance between all data and cluster centers, as well as the distance between each data point and its nearest neighbor, are measured and summed to create a new distance-based feature value to replace the original features.	<i>K</i> -NN, <i>K</i> -means	KDD '99	Recall: 80.320%	Accuracy: 80.65%
	[82]	DDoS UDP, DDoS TCP	Evaluate the practical feasibility of our method, which incorporates contextual and quantitative information of Netflow records using a specific kernel function, through experimentation on a large dataset provided by a major Internet service provider in Luxembourg.	One class SVM	Customized		Accuracy: 91.50%

	[83]	DoS, Prob	Three experiments were conducted to evaluate RT-IDS, including offline mode detection with various machine learning classification approaches, online network data for real-time intrusion detection, and post-processing procedure to enhance the detection accuracy of the IDS.	NB, DT, NN	KDD '99		NB: 78.20% DT: 99.40% NN: 98.0%
	[84]	DoS, R2L, U2R, Probe	This paper investigates IDS design by focusing on removing redundant instances, selecting relevant features using a wrapper-based approach, and implementing the proposed IDS with neuro tree for improved detection accuracy.	RF, C4.5	KDD '99		RF: 89.21% C4.5: 92.1
Unsupervised	[85]	DoS, R2L, U2R, Probe	A new method for intrusion detection is proposed, which combines (IG) and (PCA) with an ensemble classifier based on SVM, IBK, and MLP, and evaluated on three datasets (ISCX 2012, NSL-KDD, and Kyoto 2006+).	SVM, MLP, PCA	KDD '99	Precisions SVM: 87% IBK: 99.6% MLP: 82.40% Recall SVM: 90.10% IBK: 91.40% MLP: 87.201%	SVM: 85.02% IBK: 94.29% MLP: 82.42%
	[86]	DoS, R2L, U2R, Probe	A new dataset was created by combining voted outputs of built models on the GA suggested features of NSL KDD dataset based on five different labels in this study, followed by executing kernel extreme learning machine (KELM) with optimized parameters using GA.	SVM, MLP, DT, K-NN	NSL-NDD	Recall SVM: 96.81% MLP: 95.80% DT: 95.57% K-NN: 94.79%	Accuracy: SVM: 97.42% MLP: 97.02% DT: 97.14% K-NN: 96.51%

TABLE 3.4
OVERVIEW OF DL TECHNIQUES

	Ref	Attack Type	Proposed Solution	ML-Aided Technique	Dataset	Performance Evaluation Matrix	Result
Supervised	[87]	Denial of service (DoS), user to root (U2R), probe (probing), root to local (R2L)	The objective function for a single training pair in RNNs is defined as $f(\theta) = L(y_i: (y_{-i}))$ [26], where L is a distance function that measures the deviation between predictions (y_{-i}) and actual labels y_i , using a learning rate η and the number of iterations k, given a sequence of labels y_i ($i = 1, 2, \dots, m$).	Recurrent neural networks (RNN-IDS)	NSL-KDD	FPR for DoS: 2.06 R2L: 0.80 U2R: 0.07 Probe: 2.16	Accuracy of binary classification: 83.228% Accuracy of multiclassification: 81.29%
	[88]	Known genuine and malicious behavior as an attack	By using modeling network traffic as a time series based on known genuine and malicious behavior, authors improve intrusion detection, as demonstrated through training long short-term memory (LSTM) recurrent neural networks with DARPA/KDD Cup '99.	Long short-term memory (LSTM)	DARPA/KDD Cup '99		Accuracy: 93.82% and cost: 22.13
	[89]	Spam images	This paper focuses on identifying specific categories of images (e.g., adult content and political images) in email for image classification.	CNN, SVM	Customized		Accuracy: 75.10%
	[90]	Email spam	Comparing DBN and cortical algorithm DNN architectures on classification problems, CA showed higher accuracy.	Deep belief network (DBN)	Spambase		Accuracy: 96.40%

Unsupervised	[91]	Web attacks	Hybrid unsupervised detection mode by using deep-learning-based, anomaly-based web attack detection	De-noising autoencoder (DAE), stacked autoencoder (SAE), generative adversarial network (GAN), and DBM-Bi LSTM-based classification model.	CSIC2010v2	Precision: 98.78% Recall: 98.78% F1-Score: 98.78% FPR: 98.78%	Accuracy: 98%
	[92]	DoS, R2L, U2R, Probe	To address this issue, the methodology suggests subdividing connections into categories based on data volume and ensuring that all connections belonging to the same category are used either as training or as validation inputs.	Discriminative restricted Boltzmann machine (RBM)	KDD '99		The results for the experiment where the DBRM was trained and tested on the real data is 94%, and the experiment where the DBRM was trained on the KDD dataset and tested on the real data is 84–85%.
	[93]	In this paper, two assumptions are considered in regard to FDI attacks: attack stealthiness and attacker's access to measurements.	The proposed methodology involves using stacked autoencoders (SAEs) to generate multiple balanced representations of imbalanced real power system data, which are then used to train multiple random forest (RF) classifiers in parallel. The outputs of these classifiers are fused to form the input for another RF classifier, which serves as the final step in detecting attacks. The SAEs have two hidden layers of varying sizes and are equipped with a dropout layer of 30%.	Stacked autoencoders and random forest	The data used in this experiment is generated using the IEEE 14-bus, IEEE 30-bus, and IEEE 57-bus systems and the MATPOWER library.	Precision: 97.28% Recall: 89.56% F1-Score: 93.40%	Accuracy: 97.28%

TABLE 3.5
Comparison of ML and DL Techniques

	Ref	Proposed Solution					Technique	Data set	Evaluation Matrix	Reliability
Machine learning		IDS	MD	MitM	PD	SD				
	[80]	×	×	×	×	×	✓	✓	≈	×
	[81]	✓	×	×	×	×	✓	✓	≈	×
	[82]	✓	×	×	×	×	✓	✓	×	×
	[83]	✓	×	×	×	×	✓	✓	×	✓
	[84]	✓	×	×	×	×	✓	✓	×	×
	[85]	✓	×	×	×	×	✓	✓	≈	✓
	[86]	✓	×	×	×	×	✓	✓	≈	✓
Deep learning	[87]	✓	×	×	×	×	✓	✓	✓	×
	[88]	×	×	×	×	×	✓	✓	≈	×
	[89]	×	×	×	×	✓	✓	×	≈	×
	[90]	×	×	×	✓	×	✓	✓	≈	×
	[91]	×	×	×	×	×	✓	✓	✓	×
	[92]	✓	×	×	×	×	✓	✓	≈	×
	[93]	✓	×	×	×	×	✓	✓	✓	×

Table 3.5 presents a comparative analysis of different proposed solutions for intrusion detection systems (IDS), malware detection (MD), man-in-the-middle (MitM) detection, phishing detection (PD), and spam detection (SD) using ML and DL techniques. For IDS, all proposed solutions except one have achieved success in utilizing ML or DL techniques to detect intrusion. However, the reliability of these solutions varies, with some achieving comparable results to traditional techniques and others falling short. Regarding MD, none of the proposed solutions utilizing ML or DL have achieved success in detecting malware. This may suggest that traditional techniques are more effective in this area. For MitM detection, no proposed solutions have been successful in using ML or DL techniques to detect this type of attack. For PD and SD, the success rate of proposed solutions utilizing ML or DL techniques are mixed, with some achieving success while others fall short. It is important to note that, in some cases, the reliability of the proposed solution is questionable.

Looking at the Table 3.5 as a whole, it appears that traditional techniques may still be more effective in certain areas of cyber security, such as MD and MitM detection. However, the success rate of ML and DL techniques in IDS and PD/SD detection suggests that there is potential for these techniques to become more widely used in the future.

3.10 FUTURE TRENDS OF ML/DL IN CYBER SECURITY

AI and ML can be applied in almost every industry [12, 13, 94] which include education [95], tele-medicine [96–98], manufacturing [99], and cyber security [100, 101]. ML techniques easily detect cyber threats like spam [102, 103], false information

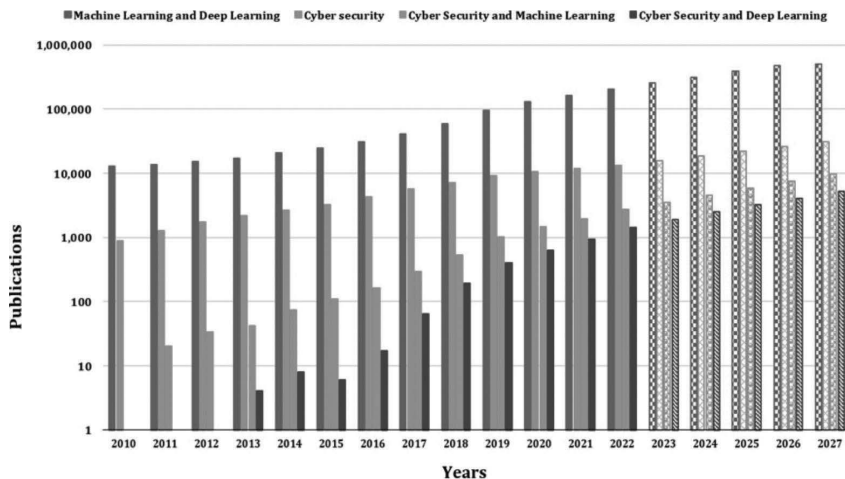


FIGURE 3.3 Publication trends of ML, DL, and cyber security.

Source: Statistics generated from Scopus publications and represented as a graph by authors.

[104, 105], abnormal data [106, 107], phishing [108, 109], and fake websites [110–114]. ML models are used to improve attack detection systems. Various researchers implemented ML techniques to identify cyber threats [111, 115]. The trend of applying ML techniques in cyber security has significantly increased in the last decade [116, 117].

In comparison with traditional techniques, they improve the quality of experience metrics [116–118]. AI-enabled data traffic monitoring techniques improve detection and response against cyber threats [116, 119]. Figure 3.3 presents the previous ten years of data related to ML and DL.

In the past few years, DL has gained more attention to process vast amounts of data and to identify more complex attack patterns [116,120]. However, ML is still widely used in cyber security, and its applications continue to evolve. Also, ML and DL models trend to identify cyber attacks in previous years [116]. ML techniques are trending as shown in Figure 3.2. Looking ahead to the period 2023–2027, it is expected that the trend of using ML and deep learning in cyber security will continue to grow. Moreover, the integration of ML with other technologies such as blockchain and the Internet of things (IoT) will provide enhanced security and privacy protection. Additionally, there will be a greater focus on explainable AI, which will enable more transparency and understanding of how ML models make decisions in cyber security [116]. Finally, as cyber threats become more advanced and sophisticated, the use of ML and deep learning will continue to be a critical tool for organizations to safeguard against cyber attacks [117–120].

3.11 CHALLENGES AND FUTURE DIRECTIONS IN APPLYING ML/DL-AIDED TECHNIQUES FOR CYBER SECURITY

A massive increase in cyber crime and malicious activities have been observed, which compromise the integrity, reliability, and confidentiality of systems in such

a way as to affect the global economy around the globe. To provide a real-time solution, ML- and DL-aided techniques play a vital role for the early detection and prevention of these types of activities. However, to obtain better results, ML and DL techniques need to be trained on the real-time datasets. In this section, different datasets for the ML and DL techniques are discussed for cyber security applications.

3.11.1 DATASET

Currently, the KDD99 dataset is widely used, but it has many limitations: Many of the available datasets are outdated, and there is a need for new datasets that are representative and balanced and that include a wide range of attack categories. Furthermore, each dataset has different numbers of features and categories, and much of the data about attacks is repetitive. ML-based techniques are used to improve overall performance, and massive data in benchmark datasets is utilized for training and testing.

Data security needs to be ensured in various applications like social media platforms and traditional databases. ML-based techniques are usually applied on a huge amount of data, which is considered a problem as well. However, some datasets usually don't include the latest or most realistic types of attacks. As a result, there is still a need to develop an exemplary and up-to-date benchmark dataset that can address these challenges. To address this issue, systematic dataset construction and incremental learning may offer viable solutions.

3.11.2 INFERIOR DETECTION ACCURACY

Another challenge is the inferior detection accuracy of machine learning methods in actual environments, where they may have used labeled datasets; the models' performance on real-world samples is not covered by the dataset.

3.11.3 EVALUATION METRICS AND REAL-TIME DETECTION COMPLEXITY

Furthermore, the real-time nature of cyber attacks is often overlooked in the literature. As cyber criminals constantly develop new attack methods to exploit network vulnerabilities, the detection rate and time complexity of intrusion detection algorithms must be considered. Efficient attack detection is critical, as false positives can lead to wasted time investigating benign activity and undermine analysts' confidence in the system. The computational complexity of machine learning models must also be considered, with frequent models' time complexity provided in Table 3.1. However, in near future, researchers are sure to be more focused on improving detection, prevention, speed, and reduction of cost.

As the field of cyber security progresses, the rate at which new attacks emerge is increasing rapidly, posing two main challenges for the application of machine learning (ML) to handle such attacks [121].

3.11.4 CONFIDENTIALITY AND PROTECTION OF DATA

Another challenge in cyber security is ensuring the confidentiality and protection of data. This creates a dilemma between securing big data and using it for security purposes [122]. Protecting data from adversarial attacks and unauthorized tampering, while still allowing legitimate users access to the data, is essential. These issues highlight the need for continued research and development of robust ML models that can adapt to evolving threats while protecting sensitive information.

3.11.5 EXPLORING THE POTENTIAL OF HYBRID METHODS FOR CYBER ATTACK DETECTION

Hybrid and multi-algorithms are considered the most effective approaches to overcoming obstacles in detection systems, such as malicious classification attacks and feature reduction. Detection systems (i.e., IDS) have been an active area of research, and hybrid detection methods have gained attention due to their promising results. These methods combine ML techniques, as described by various studies [123–125], to improve the accuracy of the detection system. However, the combination of DL and ML methods for detection systems has not been extensively explored. Also, DL algorithms are still emerging as a promising solution to computer security issues, and significant strides have been made thus far. However, DL algorithms require substantial processing power and a large amount of data, and they may suffer from overfitting, making it difficult to generalize the model and deal with gradients. These are potential research directions that could lead to even more promising results. Also, the success of AlphaGo in combining DL and traditional methods has demonstrated the potential of hybrid methods in solving complex problems, making it an exciting area of research to explore.

3.11.6 IMPROVING DETECTION SPEED AND EFFICIENCY

Improving the speed of detection is crucial in enhancing the efficiency of detection systems (i.e., IDS). This can be achieved through both algorithmic and hardware improvements [126]. However, achieving a balance between efficiency and accuracy is important, and a trade-off often exists.

One challenge in improving detection speed is the use of complex models and extensive data preprocessing methods, which can lead to low efficiency. Although most studies prioritize detection accuracy, real-time detection of attacks is essential to minimize harm. To address this issue, parallel computing using GPUs and other hardware is becoming a popular solution [125–127].

In conclusion, a combination of algorithmic and hardware improvements is necessary to enhance the speed and efficiency of detection systems (i.e., IDS). Achieving a balance between detection accuracy and efficiency is crucial in developing effective IDS that can detect attacks in real time.

Improving ML/DL algorithms is a key way to enhance the effectiveness of detection systems (i.e., IDS).

3.11.7 DESIGNING PRACTICAL MODELS

The formation of detection systems (i.e., IDS) that have real-time requirements are essential in attack detection, so they do not provide an interpretable basis for their decisions. The rise of network intrusion has prompted researchers to explore innovative approaches for improving network detection. As the field of ML and DL continues to evolve, online learning has emerged as a promising direction for the future. Online learning allows for the continuous updating of models in real time, making it ideal for dynamic environments like network IDS.

By leveraging online learning, models can be updated seamlessly as new data becomes available, thereby increasing their accuracy and efficiency in detecting potential threats. This approach eliminates the need for retraining models from scratch every time new data is introduced, saving time and resources while improving performance. In a nutshell, the use of online learning, coupled with transfer learning, represents a powerful combination for enhancing the capabilities of network IDS. As the volume and complexity of data continue to grow, the adoption of these techniques will become increasingly important for safeguarding critical network infrastructure against potential threats.

3.12 CONCLUSION

Cyber security is a growing concern worldwide, and conventional security systems are proving inadequate in detecting complex and previously unseen attacks. ML and DL techniques have emerged as a promising solution in enhancing security measures. The intersection between ML, DL, and cyber security has gained significant interest in both academia and industry, resulting in a significant increase in publications in the last decade. This chapter presents the basics of cyber security, ML, DL and provides a detailed survey of the ML and DL models by bridging the gap between the two fields in cyber security. Also, novel dataset ideas are discussed in detail. Furthermore, this chapter covers the importance of using ML- and DL-aided techniques to secure networks more accurately and also acknowledges the publication trend of past decades and future trends for the coming five years in cyber security.

REFERENCES

- [1] ICT Facts and Figures, International Telecommunication Union. *Telecommunication Development Bureau*, 2017 [Online]. Available: www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (accessed on 9 October 2019).
- [2] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer, and B. D. Payne, "Evaluating computer intrusion detection systems: A survey of common practices," *ACM Comput. Surv.*, vol. 48, no. 1, pp. 1–41, 2015.
- [3] C. N. Modi and K. Acha, "Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: A comprehensive review," *J. Supercomput.*, vol. 73, no. 3, pp. 1192–1234, 2017.
- [4] E. Viegas, A. O. Santin, A. França, R. Jasinski, V. A. Pedroni, and L. S. Oliveira, "Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems," *IEEE Trans. Comput.*, vol. 66, no. 1, pp. 163–177, Jan. 2017.

- [5] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," *Comput. Netw.*, vol. 51, no. 12, pp. 3448–3470, Aug. 2007.
- [6] The White House, Remarks by APhSCT Lisa O. Monaco at the International Conference on Cyber Security [Online]. Available: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/remarks-aphsct-lisa-o-monaco-international-conference-cyber-security> (accessed on 17 October 2019).
- [7] *10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?* [Online]. Available: <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/> (accessed on 1 June 2020).
- [8] North Atlantic Treaty Organization. *Bucharest Summit Declaration*. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest, Apr. 3, 2008 [Online]. Available: www.nato.int/cps/en/natolive/official_texts_8443.htm (accessed on 9 October 2019).
- [9] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, "Managing vulnerabilities of information systems to security incidents," in *Proc. 5th Int. Conf. Electron. Commerce (ICEC)*. ACM, Pittsburgh Pennsylvania USA, 2003, pp. 348354.
- [10] D. Craigen, N. Diakun-Thibault, and R. Purse, "Defining cybersecurity," *Technol. Innov. Manage. Rev.*, vol. 4, no. 10, pp. 1321, Oct. 2014.
- [11] I. Firdausi, C. Lim, A. Erwin, and A. S. Nugroho, "Analysis of machine learning techniques used in behavior-based malware detection," in *Proc. 2nd Int. Conf. Adv. Comput., Control, Telecommun. Technol.* IEEE, Jakarta, Indonesia, Dec. 2010, pp. 201–203.
- [12] S. Gu, B. T. Kelly, and D. Xiu, "Empirical asset pricing via machine learning," in *Proc. 31st Australas Finance Banking Conf. Chicago Booth Res. Paper 18–04, Yale ICF Working Paper 2018–09*, Sep. 2019 [Online]. Available: <https://ssrn.com/abstract=3159577>.
- [13] P. Mathur, "Overview of machine learning in finance," in *Machine Learning Applications Using Python*. Berkeley, CA: Apress, 2019, pp. 259–270 [Online]. Available: https://link.springer.com/chapter/10.1007/978-1-4842-3787-8_13.
- [14] S. Zeadally, E. Adi, Z. Baig, and I. Khan, "Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity," *IEEE Access*, vol. 8, pp. 23817–23837, 2020.
- [15] I. Wiafe, F. N. Koranteng, E. N. Obeng, N. Assyne, A. Wiafe, and S. R. Gulliver, "Artificial intelligence for cybersecurity: A systematic mapping of literature," *IEEE Access*, vol. 8, pp. 146598–146612, 2020.
- [16] A. A. Kadhim and S. B. Sadkhan, "Cognitive Radio Network Security Enhancement Based on Frequency Hopping," in *2020 Int. Conf. Adv. Sci. Eng. (ICOASE)*. IEEE, Duhok, Kurdistan Region-Iraq, 2020, pp. 1–6.
- [17] P. Louridas and C. Ebert, "Machine learning," *IEEE Softw.*, vol. 33, no. 5, pp. 110–115, Sep./Oct. 2016.
- [18] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.
- [19] A. Nassif, I. Shahin, I. Attili, M. Azzeh, and K. Shaalan, "Speech recognition using deep neural networks: A systematic review," *IEEE Access*, pp. 1–1, <http://doi.org/10.1109/ACCESS.2019.2896880>.
- [20] A. Rashid, M. J. Siddique, and S. M. Ahmed, "Machine and Deep Learning Based Comparative Analysis Using Hybrid Approaches for Intrusion Detection System," in *3rd Int. Conf. Adv. Comput. Sci. ICACS, 2020*. IEEE, Lahore, Pakistan, 2020, pp. 1–9.
- [21] R. Prasad and V. Rohokale, "Artificial intelligence and machine learning in cyber security," in *Cyber Security: The Lifeline of Information and Communication Technology*. Cham, Switzerland: Springer, 2020, pp. 231–247.

- [22] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *arXiv:1906.05799*, 2019 [Online]. Available: <http://arxiv.org/abs/1906.05799>.
- [23] K. Geis, "Machine learning: Cybersecurity that can meet the demands of today as well as the demands of tomorrow," Ph.D. dissertation, Master Sci. Cybersecur., Utica College, Utica, NY, 2019.
- [24] M. Thangavel, A. S. TGR, P. Priyadarshini, and T. Saranya, "Review on machine and deep learning applications for cyber security," in *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*. Hershey, PA: IGI Global, 2020, pp. 42–63.
- [25] R. Zebari, A. Abdulazeez, D. Zeebaree, D. Zebari, and J. Saeed, "A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction," *J. Appl. Sci. Technol. Trends*, vol. 1, no. 2, Art. no. 2, May 2020, <http://doi.org/10.38094/jastt1224>.
- [26] C. Aravindan, T. Frederick, V. Hemamalini, and M. V. J. Cathirine, "An extensive research on cyber threats using learning algorithm," *Int. Conf. Emerg. Trends Inf. Technol. Eng. ic-ETITE*, vol. 2020, pp. 1–8, 2020.
- [27] A. R. B. Gupta and J. Agrawal, "A comprehensive survey on various machine learning methods used for intrusion detection system," in *Proc.—2020 IEEE 9th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2020*. IEEE, Gwalior, India, 2020, pp. 282–289.
- [28] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (IoT) security," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646–1685, 2020.
- [29] G. E. Hinton, "Deep belief networks," *Scholarpedia*, vol. 4, no. 5, p. 5947, 2009.
- [30] D. Yu and L. Deng, "Deep learning and its applications to signal and information processing [Exploratory DSP]," *IEEE Signal Process. Mag.*, vol. 28, no. 1, pp. 145–154, Jan. 2011.
- [31] Y. Bengio, "Learning deep architectures for AI," in *Foundations Trends Machine Learning*, vol. 2, no. 1. Boston, MA: Now, 2009.
- [32] R. Collobert, J. Weston, L. Bottou, M. Karlen, K. Kavukcuoglu, and P. Kuksa, "Natural language processing (almost) from scratch," *J. Mach. Learn. Res.*, vol. 12, pp. 2493–2537, Aug. 2011.
- [33] P. Le Callet, C. Viard-Gaudin, and D. Barba, "A convolutional neural network approach for objective video quality assessment," *IEEE Trans. Neural Netw.*, vol. 17, no. 5, pp. 1316–1327, Sep. 2006.
- [34] L. F. Maimo, A. L. P. Gomez, F. J. G. Clemente, M. G. Perez, and G. M. Perez, "A self-adaptive deep learning-based system for anomaly detection in 5G networks," *IEEE Access*, vol. 6, pp. 7700–7712, 2018.
- [35] A. Abeshu and N. Chilamkurti, "Deep learning: The frontier for distributed attack detection in fog-to-things computing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 169–175, Feb. 2018.
- [36] T. M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, "Classification of malware programs using autoencoders based deep learning architecture and its application to the microsoft malware classification challenge (BIG 2015) dataset," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*. IEEE, Dayton, Ohio, USA, Jun. 2017, pp. 70–75.
- [37] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *Nature*, vol. 521, pp. 436–444, May 2015.
- [38] P. Louridas and C. Ebert, "Machine learning," *IEEE Softw.*, vol. 33, no. 5, pp. 110–115, Sep./Oct. 2016.
- [39] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245, pp. 255–260, 2015.

- [40] A. M. Kibriya, E. Frank, B. Pfahringer, and G. Holmes, "Multinomial naive Bayes for text categorization revisited," in *Proc. Australas. Joint Conf. Artif. Intell.* Berlin, Germany: Springer, 2004, pp. 488–499.
- [41] A. McCallum and K. Nigam, "A comparison of event models for naive bayes text classification," in *Proc. Workshop Learn. Text Categ. (AAAI)*, vol. 752, no. 1. Madison, WI: Citeseer, 1998, pp. 41–48 [Online]. Available: www.cs.cmu.edu/~mccallum/text-cat.html.
- [42] G. H. John and P. Langley, "Estimating continuous distributions in Bayesian classifiers," in *Proc. 11th Conf. Uncertainty Artif. Intell.* San Mateo, CA: Morgan Kaufmann, 1995, pp. 338–345.
- [43] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.
- [44] A. A. Aburomman and M. B. Ibne Reaz, "A novel SVM-kNN-PSO ensemble method for intrusion detection system," *Appl. Soft Comput.*, vol. 38, pp. 360–372, Jan. 2016.
- [45] W.-H. Chen, S.-H. Hsu, and H.-P. Shen, "Application of SVM and ANN for intrusion detection," *Comput. Oper. Res.*, vol. 32, no. 10, pp. 2617–2634, Oct. 2005.
- [46] B. Schölkopf, R. C. Williamson, A. J. Smola, J. Shawe-Taylor, and J. C. Platt, "Support vector method for novelty detection," *Proc. Adv. Neural Inf. Process. Syst.*, pp. 582–588, 2000.
- [47] A. L. Prodromidis and S. J. Stolfo, "Cost complexity-based pruning of ensemble classifiers," *Knowl. Inf. Syst.*, vol. 3, no. 4, pp. 449–469, Nov. 2001.
- [48] J. R. Quinlan, *C4. 5: Programs for Machine Learning*. Amsterdam, The Netherlands: Elsevier, 2014.
- [49] S. He, G. M. Lee, S. Han, and A. B. Whinston, "How would information disclosure influence organizations' outbound spam volume? Evidence from a field experiment," *J. Cybersecur.*, vol. 2, no. 1, pp. 99–118, Dec. 2016.
- [50] S. T. Miller and C. Busby-Earle, "Multi-perspective machine learning a classifier ensemble method for intrusion detection," in *Proc. Int. Conf. Mach. Learn. Soft Comput. (ICMLSC)*. ACM, Ho Chi Minh City, Vietnam, 2017, pp. 7–12.
- [51] A. K. Jain and R. C. Dubes, *Algorithms for Clustering Data*. Upper Saddle River, NJ: Prentice-Hall, 1988.
- [52] D. Arivudainambi, V. K. Ka, and P. Visu, "Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance," *Comput. Commun.*, vol. 147, pp. 50–57, Nov. 2019.
- [53] S. Sathasivam and W. A. T. W. Abdullah, "Logic learning in hopfield networks," *arXiv:0804.4075*, 2008 [Online]. Available: <http://arxiv.org/abs/0804.4075>.
- [54] J. M. Gómez Hidalgo, G. C. Bringas, E. P. Sánz, and F. C. García, "Content based SMS spam filtering," in *Proc. ACM Symp. Document Eng. (DocEng)*. ACM, Amsterdam, the Netherlands, 2006, pp. 107–114.
- [55] G. Jain, M. Sharma, and B. Agarwal, "Optimizing semantic LSTM for spam detection," *Int. J. Inf. Technol.*, vol. 11, no. 2, pp. 239–250, Jun. 2019.
- [56] K. Fukushima, "Neocognitron: A hierarchical neural network capable of visual pattern recognition," *Neural Netw.*, vol. 1, no. 2, pp. 119–130, Jan. 1988.
- [57] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," in *Proc. Eur. Conf. Comput. Vis.* Cham, Switzerland: Springer, 2014, pp. 818–833.
- [58] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*. IEEE, Jun. Boston, MA, USA, 2015, pp. 1–9.
- [59] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*. IEEE, Jun. 2016, pp. 770–778.

- [60] S. Lawrence, C. L. Giles, A. Chung Tsoi, and A. D. Back, "Face recognition: A convolutional neural-network approach," *IEEE Trans. Neural Netw.*, vol. 8, no. 1, pp. 98–113, Jan. 1997.
- [61] I. Wallach, M. Dzamba, and A. Heifets, "AtomNet: A deep convolutional neural network for bioactivity prediction in structure based drug discovery," *arXiv:1510.02855*, 2015 [Online]. Available: <http://arxiv.org/abs/1510.02855>.
- [62] Q. Tian, D. Han, K.-C. Li, X. Liu, L. Duan, and A. Castiglione, "An intrusion detection approach based on improved deep belief network," *Int. J. Speech Technol.*, vol. 50, no. 10, pp. 3162–3178, Oct. 2020.
- [63] G. Tzortzis and A. Likas, "Deep belief networks for spam filtering," in *Proc. 19th IEEE Int. Conf. Tools Artif. Intell. (ICTAI)*. IEEE, Patras, Greece, Oct. 2007, vol. 2, pp. 306–309.
- [64] S. Arora, R. Ge, Y. Liang, T. Ma, and Y. Zhang, "Generalization and equilibrium in generative adversarial nets (gans)," *arXiv preprint arXiv:1703.00573*, 2017.
- [65] N. Zhang, S. Ding, J. Zhang, and Y. Xue, "An overview on restricted Boltzmann machines," *Neurocomputing*, vol. 41713, pp. 0–1, 2017.
- [66] T. M. Kebede, O. Djaneye-Boundjou, B. N. Narayanan, A. Ralescu, and D. Kapp, "Classification of malware programs using autoencoders based deep learning architecture and its application to the microsoft malware classification challenge (BIG 2015) dataset," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*. IEEE, Dayton, Ohio, USA, Jun. 2017, pp. 70–75.
- [67] *DARPA1998 Dataset*, 1998. Available: www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset (accessed on 16 October 2019).
- [68] R. P. Lippmann et al., "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," in *Proc. DARPA Inf. Surv. Conf. Expo. (DISCEX)*. IEEE, South Carolina, USA, 2000, vol. 2, pp. 12–26.
- [69] *KDD99 Dataset*. 1999. Available: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (accessed on 16 October 2019).
- [70] G. Meena and R. R. Choudhary, "A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA," in *Proc. Int. Conf. Comput., Commun. Electron.* IEEE, Las Vegas, NV, USA, 2017, pp. 553–558.
- [71] M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Int. Conf. Comput. Intell. Secur. Defense Appl.* IEEE, Ottawa, Ontario, Canada, Jul. 2009, pp. 1–6.
- [72] V. Bolón-Canedo, N. Sánchez-Marroño, and A. Alonso-Betanzos, "Feature selection and classification in multiple class datasets: An application to KDD CUP 99 dataset," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 5947–5957, 2011.
- [73] *KDD99 Dataset*, 1999. Available: <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html> (accessed on 16 October 2019).
- [74] *NSL-KDD99 Dataset*, 2009. Available: www.unb.ca/cic/datasets/nsl.html (accessed on 16 October 2019).
- [75] S. Lakhina, S. Joseph, and B. Verma, "Feature reduction using principal component analysis for effective anomaly—based intrusion detection on NSL-KDD," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 6, pp. 3175–3180, 2010.
- [76] M. Xie, J. Hu, X. Yu, and E. Chang, "Evaluating host-based anomaly detection systems: Application of the frequency-based algorithms to ADFA-LD," in *Proc. Int. Conf. Netw. Syst. Secur.* Springer International Publishing, Xi'an, China, 2014, pp. 542–549.
- [77] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. 2015 Mil. Commun. Inf. Syst. Conf. (MilCIS)*, Canberra, Australia, 10–12 November 2015, pp. 1–6.

- [78] N. Moustafa and J. Slay, "The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set," *Inf. Secur. J. A, Glob. Perspect.*, vol. 25, nos. 1–3, pp. 18–31, Apr. 2016.
- [79] D. G. Mogal, S. R. Ghungrad, and B. B. Bhusare, "NIDS using machine learning classifiers on UNSW-NB15 and KDDCUP99 datasets," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 6, no. 4, pp. 533–537, Apr. 2017.
- [80] W. Yassin, N. I. Udzir, Z. Muda, and M. N. Sulaiman, "Anomaly-based intrusion detection through k-means clustering and Naives Bayes classification," in *Proc. of the 4th International Conference on Computing and Informatics (ICOCI 2013)*. Sarawak, Malaysia: Universiti Utara Malaysia, 28–30 August, 2013, (<http://www.uum.edu.my>).
- [81] W. C. Lin, S. W. Ke, and C. F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowl. Based Syst.*, 78, pp. 13–21, 2015.
- [82] C. Wagner, J. François, R. State, and T. Engel, "Machine learning approach for IP-flow record anomaly detection," In *Netw. 2011: 10th Int. IFIP TC 6 Netw. Conf., Valencia, Spain, May 9–13, 2011, Proceedings, Part I 10*. Berlin and Heidelberg: Springer, 2011, pp. 28–39.
- [83] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Comput. Commun.*, 34(18), pp. 2227–2235, 2011.
- [84] S. S. Sivatha Sindhu, S. Geetha, and A. Kannan, "Decision tree based light weight intrusion detection using a wrapper approach," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 129–141, Jan. 2012.
- [85] F. Salo, A. B. Nassif, and A. Essex, "Dimensionality reduction with IGPCA and ensemble classifier for network intrusion detection," *Comput. Netw.*, vol. 148, pp. 164–175, Jan. 2019.
- [86] J. Ghasemi, J. Esmaily, and R. Moradinezhad, "Intrusion detection system using an optimized kernel extreme learning machine and efficient features," *Sadhana*, vol. 45, no. 1, pp. 1–9, Dec. 2020.
- [87] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017, <http://doi.org/10.1109/ACCESS.2017.2762418>.
- [88] J. Kim, J. Kim, T. Thu, and H. Kim, "Long short term memory recurrent neural network classifier for intrusion detection," in: *Proc. Int. Conf. Platf. Technol. Serv. (PlatCon)*. IEEE, Jeju, South Korea, 2016, pp. 1–5.
- [89] E.-X. Shang and H.-G. Zhang, "Image spam classification based on convolutional neural network," in *Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC)*. IEEE, Jeju Island, South Korea, Jul. 2016, vol. 1, pp. 398–403.
- [90] Y. Rizk, N. Hajj, N. Mitri, and M. Awad, "Deep belief networks and cortical algorithms: A comparative study for supervised classification," *Appl. Comput. Inform.*, vol. 15, no. 2, pp. 81–93, 2019.
- [91] S. Pillai and A. Sharma, "Hybrid unsupervised web-attack detection and classification—A deep learning approach," *Comput. Stand. Interfaces*, p. 103738, 2023.
- [92] U. Fiore, F. Palmieri, A. Castiglione, and A. De Santis, "Network anomaly detection with the restricted Boltzmann machine," *Neurocomputing*, vol. 122, pp. 13–23, 2013.
- [93] A. Al-Abassi, J. Sakhnini, and H. Karimipour, "Unsupervised stacked autoencoders for anomaly detection on smart cyber-physical grids," in *2020 IEEE Int. Conf. Syst. Man Cybernet. (SMC)*. IEEE, Oct. 2020, pp. 3123–3129.
- [94] S. Emerson, R. Kennedy, L. O'Shea, and J. O'Brien, "Trends and applications of machine learning in quantitative finance," in *Proc. 8th Int. Conf. Econ. Finance Res. (ICEFR)*, 2019, pp. 1–9, [Online]. Available SSRN: <https://ssrn.com/abstract=3397005>.

- [95] K. Shaukat et al., “Student’s performance in the context of data mining,” in *Proc. 19th Int. Multi-Topic Conf. (INMIC)*. IEEE, Islamabad, Pakistan, 2016.
- [96] S. Jha and E. J. Topol, “Adapting to artificial intelligence: Radiologists and pathologists as information specialists,” *Jama*, vol. 316, no. 22, pp. 2353–2354, 2016.
- [97] A. I. Tekkesin, “Artificial intelligence in healthcare: Past, present and future,” *Anatolian J. Cardiol.*, vol. 2, no. 4, pp. 230–243, 2019.
- [98] K. Shaukat, N. Masood, A. Bin Shafaat, K. Jabbar, H. Shabbir, and S. Shabbir, “Dengue fever in perspective of clustering algorithms,” *arXiv:1511.07353*, 2015 [Online]. Available: <http://arxiv.org/abs/1511.07353>.
- [99] B.-H. Li, B.-C. Hou, W.-T. Yu, X.-B. Lu, and C.-W. Yang, “Applications of artificial intelligence in intelligent manufacturing: A review,” *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 1, pp. 86–96, 2017.
- [100] C. Virmani, T. Choudhary, A. Pillai, and M. Rani, “Applications of machine learning in cyber security,” in *Handbook of Research on Machine and Deep Learning Applications for Cyber Security*. Hershey, PA: IGI Global, 2020, pp. 83–103.
- [101] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, and J. Li, “Performance comparison and current challenges of using machine learning techniques in cybersecurity,” *Energies*, vol. 13, no. 10, p. 2509, May 2020.
- [102] A. A. Alurkar, S. B. Ranade, S. V. Joshi, S. S. Ranade, G. R. Shinde, P. A. Sonewar, and P. N. Mahalle, “A comparative analysis and discussion of email spam classification methods using machine learning techniques,” in *Applied Machine Learning for Smart Data Analysis*. Boca Raton, FL: CRC Press, May 2019, p. 225 [Online]. Available: https://books.google.com.au/books?id=iKWaDwAAQBAJ&dq=A+comparative+analysis+and+discussion+of+email+spam+classification+methods+using+machine+learning+tech+2019+niques.&lr=&source=gbs_navlinks_s.
- [103] A. K. Jain, D. Goel, S. Agarwal, Y. Singh, and G. Bajaj, “Predicting spam messages using back propagation neural network,” *Wireless Pers. Commun.*, vol. 110, no. 1, pp. 403–422, Jan. 2020.
- [104] D. Prusti, S. S. Padmanabhuni, and S. K. Rath, “Credit card fraud detection by implementing machine learning techniques,” *Tech. Rep.*, 2019, pp. 1–10 [Online]. Available: <http://dspace.nitrkl.ac.in/dspace/handle/2080/3273>.
- [105] M. Lokanan, V. Tran, and N. H. Vuong, “Detecting anomalies in financial statements using machine learning algorithm,” *Asian J. Accounting Res.*, vol. 4, no. 2, pp. 181–201, Oct. 2019.
- [106] Z. Ma, H. Ge, Y. Liu, M. Zhao, and J. Ma, “A combination method for Android malware detection based on control flow graphs and machine learning algorithms,” *IEEE Access*, vol. 7, pp. 21235–21245, 2019.
- [107] D. Sahoo, C. Liu, and S. C. H. Hoi, “Malicious URL detection using machine learning: A survey,” *arXiv:1701.07179*, 2017 [Online]. Available: <http://arxiv.org/abs/1701.07179>.
- [108] R. S. Rao and A. R. Pais, “Detection of phishing websites using an efficient feature-based machine learning framework,” *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3851–3873, Aug. 2019.
- [109] O. K. Sahingoz, E. E. Huber, O. Demir, and B. Diri, “Machine learning based phishing detection from URLs,” *Expert Syst. Appl.*, vol. 117, pp. 345–357, Mar. 2019.
- [110] M. Almukaynizi, A. Grimm, E. Nunes, J. Shakarian, and P. Shakarian, “Predicting cyber threats through the dynamics of user connectivity in darkweb and deepweb forums,” *ACM Comput. Social Sci.*, 2017 [Online]. Available: <https://usc-isi-i2.github.io/papers/kristina02.pdf>.
- [111] M. Almukaynizi, A. Grimm, E. Nunes, J. Shakarian, and P. Shakarian, “Predicting cyber threats through hacker social networks in darkweb and deepweb forums,” in *Proc. Int. Conf. Comput. Social Sci. Soc. Americas (CSSS)*. ACM, Santa Fe NM USA, 2017, pp. 1–7.

- [112] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019.
- [113] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102419.
- [114] M. Pradhan, C. K. Nayak, and S. K. Pradhan, "Intrusion detection system (IDS) and their types," in *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global, 2020, pp. 481–497.
- [115] S. Sarkar, M. Almkaynizi, J. Shakarian, and P. Shakarian, "Predicting enterprise cyber incidents using social network analysis on dark Web hacker forums," *Cyber Defense Rev.*, pp. 87–102, Mar. 2019.
- [116] K. Shaukat, Kamran, et al. "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.
- [117] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, "Darknet and deepnet mining for proactive cybersecurity threat intelligence," in *Proc. IEEE Conf. Intell. Secur. Informat. (ISI)*. IEEE, Tucson, Arizona, USA, Sep. 2016, pp. 7–12.
- [118] M. Kadoguchi, S. Hayashi, M. Hashimoto, and A. Otsuka, "Exploring the dark Web for cyber threat intelligence using machine learning," in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*. IEEE, Shenzhen, China, Jul. 2019, pp. 200–202.
- [119] X. Zhang and K. Chow, "A framework for dark Web threat intelligence analysis," in *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications*. Hershey, PA: IGI Global, 2020, pp. 266–276.
- [120] R. Prasad and V. Rohokale, "Artificial intelligence and machine learning in cyber security," in *Cyber Security: The Lifeline of Information and Communication Technology*. Cham, Switzerland: Springer, 2020, pp. 231–247.
- [121] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy*. IEEE, Berkeley, USA, May 2010, pp. 305–316.
- [122] A. A. Cárdenas, P. K. Manadhata, and S. P. Rajan, "Big data analytics for security," *IEEE Secur. Priv.*, vol. 11, no. 6, pp. 74–76, Nov./Dec. 2013.
- [123] M. S. Pervez and D. M. Farid, "Feature selection and intrusion classification in NSL-KDD CUP 99 dataset employing SVMs," in *Proc. 8th Int. Conf. Softw., Knowl., Inf. Manage. Appl. (SKIMA)*. IEEE, Dhaka, Bangladesh, 2014, pp. 1–6.
- [124] R. T. Kokila, S. T. Selvi, and K. Govindarajan, "DDoS detection and analysis in SDN-based environment using support vector machine classifier," in *Proc. 6th Int. Conf. Adv. Comput.* IEEE, Swissotel, Kolkata, India, 2015, pp. 205–210.
- [125] E. G. Dada, "A hybridized SVM-kNN-pdAPSO approach to intrusion detection system," in *Proc. Fac. Seminar Ser.*, vol. 8, University of Maiduguri Faculty of Engineering Seminar Series, Maiduguri, Nigeria, 2017, pp. 14–21.
- [126] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced Intrusion Detection System," in *Proc. 2016 IEEE 21st Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Berlin, Germany, 6–9 Sept. 2016, pp. 1–8.
- [127] P. Kuttranont, K. Boonprakob, C. Phaudphut, S. Permpol, P. Aimtongkhamand, U. KoKaew, B. Waikham, and C. So-In, "Parallel KNN and neighborhood classification implementations on GPU for network intrusion detection." *J. Telecommun. Electron. Comput. Eng. (JTEC)*, vol. 9, pp. 29–33, 2017.

4 AI-Based Secure Wireless Communication Technologies and Cyber Threats for IoT Networks

Usman Haider, Bakhtawar Nawaal, Inam Ullah Khan, and Salma El Hajjami

4.1 INTRODUCTION

Artificial intelligence (AI) has opened countless opportunities to mankind, and each of them contains a world in itself. Researchers are exploring where humans can benefit from these new emerging technologies. AI is applicable in almost every segment of life. However, autonomous vehicles are considered one such recent application in this field of study [1]. Tesla is renowned for introducing driver-less cars. Further, AI-enabled medicines are very helpful in pandemic. Therefore, due to artificial intelligence, the detection and diagnosis of many deadly diseases are made possible. Various diseases are now being diagnosed by systems based on AI. Also, cancerous/tumorous cells are easily monitored using AI models that are used to decrease the fatality rate [2, 3]. Moreover, AI has found many applications in cardiology, neurology, and dermatology. For the purpose of data and information security, end devices are used to safeguard overall networks from intrusion. More interestingly, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) powered by artificial intelligence can easily detect threats [4, 5]. All industries are on their way to automation because AI has created a lot of room for progress [6]. AI tools are much in demand because they easily can make timely decisions. AI-based systems are comprised of wireless sensor nodes that constantly monitor factors related to crops [7]. Figure 4.1 demonstrates the use of artificial intelligence in cyber security, autonomous vehicles, ad hoc networks, healthcare, agriculture, and voice assistants.

Wireless communication networks received attention from day one. Now the world is about to launch sixth generation (6G) wireless networks commercially, which are going to transform the world into a newer place. Automation is necessary in the modern world; it drives AI-enabled networks to achieve various goals [8]. Wireless communication networks use wireless channels for a variety of communication needs [9, 10]. Advance networks are used in television, radio broadcasting,

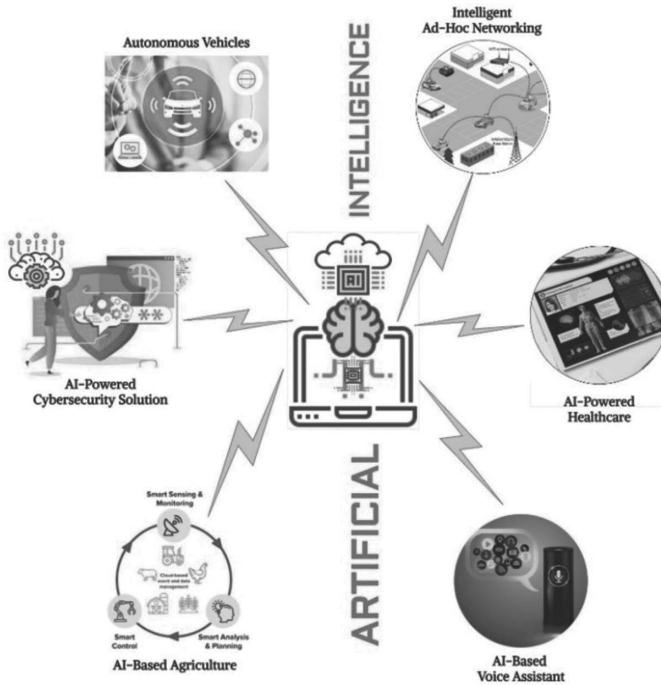


FIGURE 4.1 Uses of artificial intelligence (AI).

satellite communication, radar, mobile telephone system (cellular communication), global positioning system (GPS), infrared communication, WLAN (Wi-Fi), and Bluetooth. Recently, wireless sensor node (WSN) and ad hoc communication networks are trending topics that researchers are keenly working on. Wireless sensor networks (WSN) are using cost-effective IoT devices [11]. However, ad hoc networks use wireless communication technologies for better signal strength. Therefore, there are different types of ad hoc networks, which include MANET, FANET, RANET, and VANET [12]. Due to artificial intelligence, wireless technologies are improved with the passage of time, and AI-powered wireless communication systems are in demand.

As mentioned earlier, the latest proposition for wireless communication is 6G. Transfer learning (TL) is a novel approach for 6G networks, which reveal new domains to learn from previous events and to apply on wireless communication fields [13]. 6G-enabled quantum computing will eliminate error and provide solutions to existing problems [14]. Many issues have been encountered, and the most critical one is performance of both machine learning (ML) algorithms and wireless networks [15]. More interestingly, high accuracy in machine learning classifiers needs to be balanced. However, in machine learning high accuracy, false alarm, precision, recall, support, and F1-score need to be properly improved for achieving high standards of automation.

The deficiencies to be discussed need to be addressed by researchers and can be significant in their contribution. In addition, especially with regard to artificial intelligence, governments are planning to pass better legislation for machine learning. Further, as the machine learning industry is growing day by day with AI, ethics will play an ever greater role in the smart world [16–18].

4.2 LITERATURE STUDY

This section provides a brief literature study regarding AI-enabled wireless communication techniques.

Meta-heuristic search technique is basically subpart of artificial intelligence. Therefore, ant colony optimization protocol using wireless communication networks is deployed in flying ad hoc networks. Comparative analysis is performed to check the performance of AntHocNet with other traditional routing protocols. Moreover, end-to-end delay is the major problem found during communication [19]. Accordingly, Inam Ullah Khan et al. has proposed a novel routing protocol called E-AntHocNet which is used to improve energy efficiency within UAV networks. The random way point (RWP) model is used to check the behavior of unmanned aerial vehicles [20]. Existing mobility models of MANETs are used in UAV networks; therefore hybrid models need to be designed. IoT networks are having many issues, especially with signal strength from base station to IoT nodes, and, as a result, machine learning classifiers improve communication standards within nodes. The internet of flying vehicles used to have limited mobility due to wireless connectivity [21].

Three-dimensional modeling improves signal strength measurement in IoT connected networks. Both indoor and outdoor scenarios are used for node localization. For location tracking of IoT nodes, localization is quite helpful. Similarly, work needs to be done in real-time environments to improve the received signal strength indicator [22]. IoT-enabled UAVs are seeing application in real-time modeling in health and sports. Therefore, routing protocols play an important role during overall communication within nodes [23]. Seema Begum et al. introduced a new approach, which is based on cognitive modeling for IoT networks. Further, security needs to be ensured for IoT networks. As a result, Markov-chain-enabled IDSs are designed to detect DoS, DDoS, and ping of death attacks [24, 25]. Sajid, Faiqa, et al. [26] proposed a IoT-based methodology for the classification of heart rate data for the prevention of heart attacks using a machine learning technique through a generated dataset secured by RSA encryption. However, the data rates are slow due to RSA because it involves large numbers.

Khan, Inam Ullah, et al. [27] explained the dynamic behavior of UAVs, proposed an unmanned aerial-AntHocNet protocol, and compared it with other modern routing protocols using a random way mobility model and achieved good results. As only one mobility model is being used in experimentation, the results on other models remain undefined, and the communication standard can be compromised. Khan, Inam Ullah, et al. [28] proposed an improved sequencing heuristic DSDV (ISH-DSDV) protocol to address the energy problems in aerial vehicles. Table 4.1 depicts various artificial intelligence approaches with limitations.

TABLE 4.1**Different AI-Based Approaches in Wireless Communication with Limitations**

Reference	Technique Used	Description	Limitations
[29]	DNN	This work used DNNs to for various wireless communication processes, i.e., channel modeling, channel encoding/decoding signal detection, etc.	These use of DNN in wireless communication make it vulnerable to various kind of attacks.
[30]	<i>K</i> -NN, SVM algorithms	This paper proposed multiclass classification for the selection of antenna using machine learning.	In <i>K</i> -NN, it is very difficult to designate the correct value of <i>K</i> , and somehow it is computationally not efficient enough.
[31]	Federated learning (FL)	This work proposed collaborative federated learning (CFL), based on distributed ML, for optimized performance.	In FL, the use of unsupervised algorithms is preferred, and some limitations crop up during data cleaning and labeling.
[32]	DNN	This paper proposed the used of deep learning for optical wireless communication to counter various design challenges.	The system training used is very slow.
[33]	CNNs, FNNs, RF, and GRUs	This work tried to address the channel assignment problems in wireless communication using ML algorithms and convex optimization-based algorithms.	The system is not very efficient in the case of larger numbers of users and sub-channels.
[34]	DNN	This work proposed deep neural networks for IDS using cross-correlation process and compared performance with some other ML algorithms.	The accuracy of the system significantly low much better system available.
[35]	ANN	The paper proposed the use of ML for extremely low latency for next-generation wireless communication.	The application of ANNs is significantly time-consuming and computationally expensive.
[36]	DT	This work described the benefits of ML in wireless communication in relay selection through multiclass classification.	The implementation of DT is quite expensive, involving repetitive training as well as having higher complexity.
[37]	Distributed batch gradient descent (DBGD)	This research proposed a novel approach for D2D communication with better accuracy and reduced training delay.	Gradient descent (GD) occupies some mathematical limitations.
[38]	RF, AB, GBM, XGB, and ETC	This work presented an assessment study of seven ML algorithms for an efficient anomaly-based IDS using three datasets for learning and also evaluated the performance through Raspberry-Pi.	Anomaly-based IDS usually has a significantly high false alarm rate.

4.3 AI FOR NEXT-GENERATION WIRELESS NETWORKS

Wireless communication can be made possible from sender to receiver using various media. In the first generation of wireless communication, analogue communication was the backbone, which was later changed to digital in the second generation (2G) with the evolution of GSM. However, 3G technology has a working scenario of circuit switching through UMTS using different techniques of CDMA. Fourth-generation communication networks are based on circuit switching and packet switching. More interestingly, 5G works mainly on packet switching [39–41]. Sixth-generation communications have improved channels in next-generation intelligent networks. In comparison with 5G networks, 6G is much more advanced [42]. Some researchers have called AI a “double-edged sword” in sixth generation of wireless communication due to the network’s threat resistance and end-to-end automation [43]. AI is serving as a base in 6G for many modern technologies like smart computing, augmented reality, extended reality (XR), etc. [44]. For short distances, optical

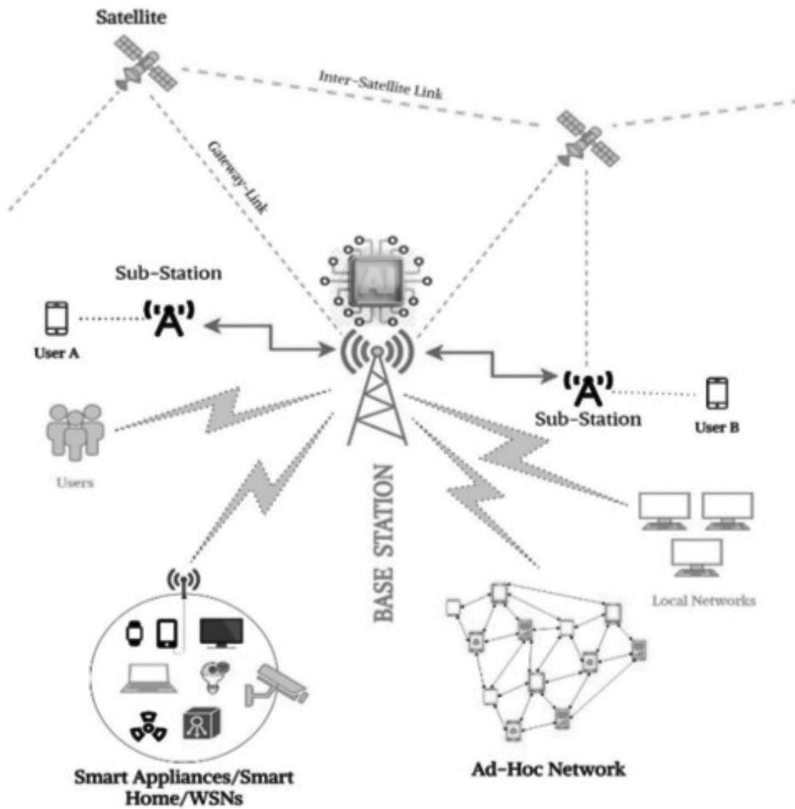


FIGURE 4.2 AI-based wireless communication.

wireless (OW) communication is an excellent approach with a speed in the range of gigabytes per second. Moreover, the different techniques of deep learning (DL) are being used to deal with many parametrical complications [45, 46]. Figure 4.2 displays a sketch of modern AI-based wireless communication system.

4.4 APPLICATIONS OF AI FOR SMART COMPUTING

The definition of smart computing is hidden in itself as “SMART”: self-monitoring, analysis, and reporting technology. It is used to monitor and detect any hardware failure in a system automatically and was first used for the following application with hard drives. Smart computing emerged to be an intelligent technology due to the integration of AI. AI powered the smart computing, and it is deployed in many applications. In smart computing, AI is used in smart houses, smart grid, smart agriculture, smart healthcare, smart cyber security, smart networking, smart vehicles, etc.

4.4.1 SMART HOUSE

Smart house is a building block of smart cities. Smart houses consist of intelligent appliances like smart air conditioners, smart TVs, smart refrigerators, smart lights, smart fans, etc. A smart house enables you to monitor the house 24 hours a day and to control all its gadgets remotely [47]. You can have a check on home security, and you can turn on the AC or a heater before coming home on a hot or cold day, respectively. Thus smart computing makes your house secure and comfortable.

4.4.2 SMART GRID

A smart grid is a digital electricity network used to distribute electricity through two-way digital communication. It has various advantages over a conventional grid system as it is more efficient, transparent, and reliable, and it reduces the consumption as well as the cost of electricity [48]. It is also environment friendly and very flexible in applications. Smart grid is composed of three types of systems: (1) smart infrastructure system, (2) smart management system, (3) smart protection system [49].

4.4.3 SMART NETWORKING AND SECURITY

AI has also opened doors for intelligent networking. Devices on both ends learn the path that would be feasible for the communication depending on the applied protocol. Cyber security has been the main focus in AI, and various novel techniques have been introduced in the security of networks. Intrusion detection system (IDS) and intrusion prevention system (IPS) have been powered with AI. They are trained properly using appropriate ML algorithms for the possible kinds of attack, are also made intelligent enough to detect zero-day exploitation, and are programmed to take action automatically in case of intrusion [50, 51]. In signature-based IDS, the attack signature is already saved and possible threats are matched, and in anomaly-based IDS, the system is trained to sense attack in real environments using the knowledge of a training dataset [52, 53].

4.4.4 SMART HEALTHCARE

Healthcare has grown rapidly with the integration of artificial intelligence and internet of things (IoT). The increasing number of chronic diseases have led researchers to use the latest technologies in healthcare for the diagnosis and treatment and to control the patient's critical condition. Patients can be under supervision anywhere through various devices accessed through doctor's workstation, and AI has made the machines intelligent enough to sound the alarm for any emergency depending on parameters, under supervision and by means of various sensors. In smart healthcare, a patient's affected organ is tested for every kind of threat automatically with optimal diagnosis that might have been missed in a doctor's examination [54, 55].

4.4.5 SMART AGRICULTURE

Agriculture has been made smarter with the use of AI and IoT. Wireless sensor nodes (WSNs) have found a huge application in smart agriculture. The network of WSNs is energized with AI over intelligent decisions depending on the circumstances. AI has provided the farmers with pest control at a very early stage in order to prevent damage to crops. The irrigation system can be not only controlled remotely but also automated via sensor readings. Even robots can be used to sow seeds and reap crops. Thus, AI in smart agriculture allows the efficient management of all agricultural resources [56, 57].

4.5 AI FOR CYBER SCIENCE

Some of the famous attacks are denial of service (DoS), distributed denial of service (DDoS), phishing attack, ping of death, ransomwares, man-in-the-middle attack, SQL injection, malware, etc. In the past, some very huge cyber attacks occurred that directly affected the privacy and finances of the public as well as of companies [58]. Previously, only malware could be detected because the developer had its identity and could be easily identified through signature detection, but unknown threats might not be detected, leading the way to the evolution of anomaly detection [59]. AI-based solutions have boomed in the security industry with a variety of efficient solutions. Some works proposed the use of AI in intelligent detection and prevention through artificial police agents in a decentralized fashion, creating an artificial immune system like the human body [60]. Some researchers have used ML-based IDS, IPS, firewalls, etc. for efficient network security even against zero-day exploit. AI also proposes the cloud-based security solutions [61, 62]. Thus, with the introduction of AI in cyber science, the critical infrastructure is more secure than with older security solutions.

4.6 CYBER THREATS

There are numerous cyber threats in today's era, each of which has multiple types. Some of the famous cyber attacks are discussed here.

4.6.1 DENIAL OF SERVICE (DoS) ATTACK

This is the most famous, common, and deadly attack. In this attack, the attacker's sole intention is to keep the target down from its services, and even legal users are unable to connect to the server. A huge amount of traffic is sent by the attacker to the victim, who is unable to handle it, which takes the server down completely [63] (Figure 4.3).

4.6.2 DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK

DDoS is a type of DoS that can be considered an advanced and more destructive version of DoS. The intention of the attacker is same but with a different approach. The attacker uses various compromised PCs/systems to ping the victim through various parts of world, thus generating a huge amount of traffic and dismantling the up state of victim [64].

4.6.3 DOMAIN NAME SYSTEM (DNS) ATTACK

A DNS attack targets the DNS service of the network, thus compromising its sustainability and availability. It can slow down the web server, thus affecting its ranking. It redirects the network traffic to a malicious website instead of to the legitimate website by changing the IP address in DNS server, thereby corrupting it. A DNS attack is usually done through cache poisoning [65]. A DNS attack is shown in Figure 4.4.

4.6.4 SYBIL ATTACK

The intruder using the Sybil tries to own the network through variously active false identities by a single node. It is an especially serious threat to a peer-to-peer network because the hacker is pretending to be many persons at the same time and can fully control the network. Usually, Sybil attacks are carried out the Tor network. According to studies, category accounts for 51% of the attacks in blockchain networks [66]. The fake reviews and comments on e-commerce websites like Amazon are an example of Sybil attacks. Figure 4.5 shows a sketch of a Sybil attack.

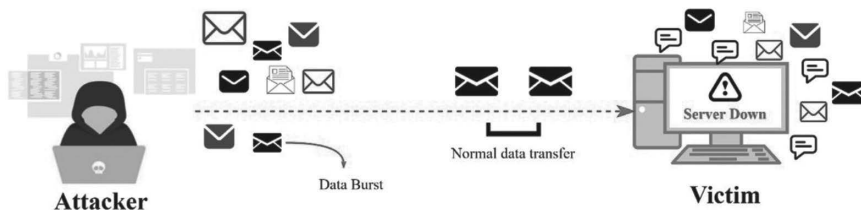


FIGURE 4.3 Denial of service attack (DoS).

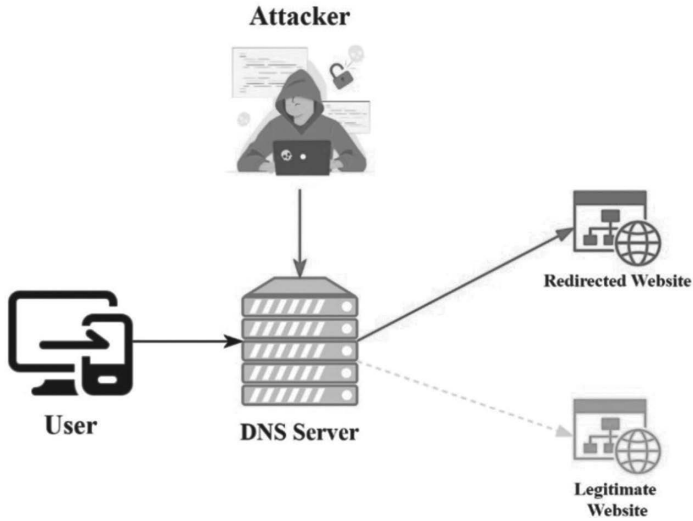


FIGURE 4.4 Domain name system attack.

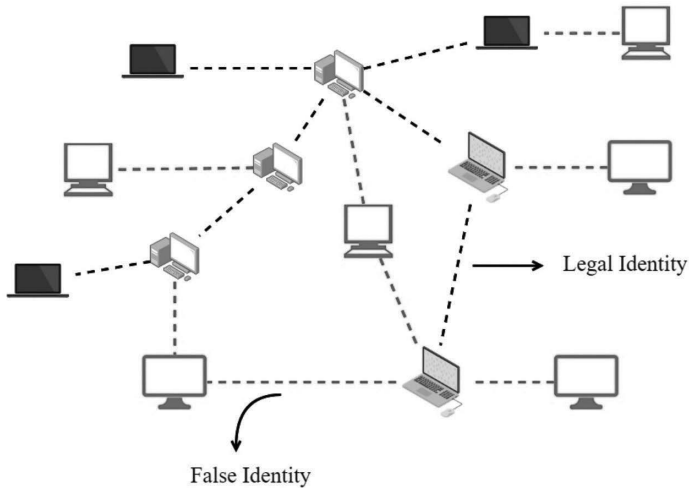


FIGURE 4.5 Sketch of Sybil attack.

4.6.5 PING OF DEATH (POD) ATTACK

In this kind of attack, the attacker tries to freeze and destabilize the victim by sending malfunctioned or oversized packets. The attacker uses the hit-and-trial method to get to know the system’s limit by continuously sending packets. As the attacker exceeds the system limits, the system becomes unable to process beyond functional-packet-sized and stops responding. Some researchers call the PoD a kind of DoS and DDoS attack [67]. Figure 4.6 describes the idea of PoD attack.

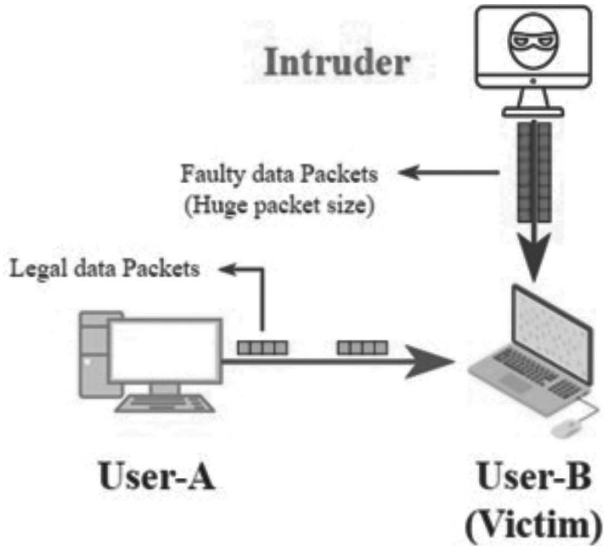


FIGURE 4.6 Ping of death attack.

4.7 FUTURE DIRECTIONS

In near future, everything is going to be smart, making security a serious problem. This critical problem is addressed by artificial intelligence, machine learning, big data, evolutionary computing, ant colony optimization, genetic algorithm, etc. Thus the researchers working on smart gadgets and IoTs should also work on their security and threat resistance as well. Moreover, security solutions with more accurate results are needed [68–70].

4.8 CONCLUSION

The technology is going to surpass 24 hours supervision in very near future, and artificial intelligence is the key to the new transformation. However, applications of AI are countless because an intelligent system can be deployed anywhere and efficiently perform any assigned task if trained properly. Nowadays, everyone has a wireless device in his/her pocket and is connected with the huge communication system of a smart world. Wireless systems include base stations for local and national-level communication, as well as satellites on the national and international levels. AI in collaboration with wireless communication is going to change world dynamics and will give rise to smart computing. In short, the future is very bright on this planet through AI practices in intelligent systems, thus forming an entirely smart world.

REFERENCES

- [1] Abdul Jabbar, Rusul, et al. "Applications of artificial intelligence in transport: An overview." *Sustainability* 11.1 (2019): 189.

- [2] Nichols, James A., Hsien W. Herbert Chan, and Matthew A. B. Baker. "Machine learning: Applications of artificial intelligence to imaging and diagnosis." *Biophysical Reviews* 11.1 (2019): 111–118.
- [3] Subhan, Fazal, et al. "Cancerous tumor controlled treatment using search heuristic (GA)-based sliding mode and synergetic controller." *Cancers* 14.17 (2022): 4191.
- [4] Kumar, Gulshan, and Krishan Kumar. "The use of artificial-intelligence-based ensembles for intrusion detection: A review." *Applied Computational Intelligence and Soft Computing* 2012 (2012).
- [5] Yildirim, Merve. "Artificial intelligence-based solutions for cyber security problems." *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems. IGI Global* (2021): 68–86.
- [6] Battina, Dhaya Sindhu. "Application research of artificial intelligence in electrical automation control." *International Journal of Creative Research Thoughts (IJCRT), ISSN* (2015): 2320–2882.
- [7] Eli-Chukwu, Ngozi Clara. "Applications of artificial intelligence in agriculture: A review." *Engineering, Technology & Applied Science Research* 9.4 (2019): 4377–4383.
- [8] You, Xiaohu, et al. "Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts." *Science China Information Sciences* 64.1 (2021): 1–74.
- [9] Stallings, William. *Wireless Communications & Networks*. Pearson Education India, 2009.
- [10] Li, Xichun, et al. "The future of mobile wireless communication networks." *2009 International Conference on Communication Software and Networks*. IEEE, 2009.
- [11] García-Hernández, Carlos F., et al. "Wireless sensor networks and applications: A survey." *IJCSNS International Journal of Computer Science and Network Security* 7.3 (2007): 264–273.
- [12] Xu, Bangnan, Sven Hischke, and Bernhard Walke. "The role of ad hoc networking in future wireless communications." *International Conference on Communication Technology Proceedings, 2003. ICCT 2003*. Vol. 2. IEEE, 2003.
- [13] Wang, Meiyu, et al. "Transfer learning promotes 6G wireless communications: Recent advances and future challenges." *IEEE Transactions on Reliability* 70.2 (2021): 790–807.
- [14] Akyildiz, Ian F., Ahan Kak, and Shuai Nie. "6G and beyond: The future of wireless communications systems." *IEEE Access* 8 (2020): 133995–134030.
- [15] Groumpos, Peter P. "Artificial intelligence: Issues, challenges, opportunities and threats." *Conference on Creativity in Intelligent Technologies and Data Science*. Springer, 2019.
- [16] Ghallab, Malik. "Responsible AI: Requirements and challenges." *AI Perspectives* 1.1 (2019): 1–7.
- [17] Rodrigues, Rowena. "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities." *Journal of Responsible Technology* 4 (2020): 100005.
- [18] Borenstein, Jason, and Ayanna Howard. "Emerging challenges in AI and the need for AI ethics education." *AI and Ethics* 1.1 (2021): 61–65.
- [19] Khan, Inam Ullah, et al. "Reinforce based optimization in wireless communication technologies and routing techniques using internet of flying vehicles." *The 4th International Conference on Future Networks and Distributed Systems (ICFNDS)*. ACM, 2020, pp. 1–6.
- [20] Khan, Inam Ullah, et al. "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)." *IEEE Access* 8 (2020): 56371–56378.

- [21] Khan, Inam Ullah, et al. "Routing protocols & unmanned aerial vehicles autonomous localization in flying networks." *International Journal of Communication Systems* (2021): e4885.
- [22] Khan, Inam Ullah, et al. "RSSI-controlled long-range communication in secured IoT-enabled unmanned aerial vehicles." *Mobile Information Systems* 2021 (2021).
- [23] Khan, Inam Ullah, et al. "Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing." *Journal of Healthcare Engineering* 2021 (2021).
- [24] Khan, Inam Ullah, et al. "Intelligent detection system enabled attack probability using Markov chain in aerial networks." *Wireless Communications and Mobile Computing* 2021 (2021).
- [25] Begum, Seema, et al. "Source routing for distributed big data-based cognitive internet of things (CIoT)." *Wireless Communications and Mobile Computing* 2021 (2021).
- [26] Sajid, Faiqa, et al. "Secure and efficient data storage operations by using intelligent classification technique and RSA algorithm in IoT-based cloud computing." *Scientific Programming* 2022 (2022).
- [27] Khan, Inam Ullah, et al. "A novel design of FANET routing protocol aided 5G communication using IoT." *Journal of Mobile Multimedia* (2022): 1333–1354.
- [28] Khan, Inam Ullah, et al. "Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS." *Computers, Materials and Continua* 70.2 (2022): 3653–3666.
- [29] Wang, Jun, et al. "Artificial intelligence and wireless communications." *Frontiers of Information Technology & Electronic Engineering* 21.10 (2020): 1413–1425.
- [30] Joung, Jingon. "Machine learning-based antenna selection in wireless communications." *IEEE Communications Letters* 20.11 (2016): 2241–2244.
- [31] Chen, Mingzhe, et al. "Wireless communications for collaborative federated learning." *IEEE Communications Magazine* 58.12 (2020): 48–54.
- [32] Lee, Hoon, et al. "Deep learning framework for wireless systems: Applications to optical wireless communications." *IEEE Communications Magazine* 57.3 (2019): 35–41.
- [33] Jia, Guangyu, et al. "Channel assignment in uplink wireless communication using machine learning approach." *IEEE Communications Letters* 24.4 (2020): 787–791.
- [34] Gowdhaman, V., and R. Dhanapal. "An intrusion detection system for wireless sensor networks using deep neural network." *Soft Computing* 26.23 (2022): 13059–13067.
- [35] Chen, Mingzhe, et al. "Artificial neural networks-based machine learning for wireless networks: A tutorial." *IEEE Communications Surveys & Tutorials* 21.4 (2019): 3039–3071.
- [36] Jagannath, Anu, Jithin Jagannath, and Tommaso Melodia. "Redefining wireless communication for 6G: Signal processing meets deep learning with deep unfolding." *arXiv preprint arXiv:2004.10715* (2020).
- [37] Cai, Xiaoran, et al. "D2D-enabled data sharing for distributed machine learning at wireless network edge." *IEEE Wireless Communications Letters* 9.9 (2020): 1457–1461.
- [38] Verma, Abhishek, and Virender Ranga. "Machine learning based intrusion detection systems for IoT applications." *Wireless Personal Communications* 111.4 (2020): 2287–2310.
- [39] Sharma, Pankaj. "Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network." *International Journal of Computer Science and Mobile Computing* 2.8 (2013): 47–53.
- [40] Vora, Lopa J. "Evolution of mobile generation technology: 1G to 5G and review of upcoming wireless technology 5G." *International Journal of Modern Trends in Engineering and Research* 2.10 (2015): 281–290.

- [41] Gawas, Anju Uttam. "An overview on evolution of mobile wireless communication networks: 1G–6G." *International Journal on Recent and Innovation Trends in Computing and Communication* 3.5 (2015): 3130–3133.
- [42] Yang, Ping, et al. "6G wireless communications: Vision and potential techniques." *IEEE Network* 33.4 (2019): 70–75.
- [43] Siriwardhana, Yushan, et al. "AI and 6G security: Opportunities and challenges." *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021.
- [44] Ahammed, Tareq Bin, and Ripon Patgiri. "6G and AI: The emergence of future forefront technology." *2020 Advanced Communication Technologies and Signal Processing (ACTS)*. IEEE, 2020.
- [45] Borah, Deva K., et al. "A review of communication-oriented optical wireless systems." *EURASIP Journal on Wireless Communications and Networking* 2012 (2012): 1–28.
- [46] Lee, Hoon, et al. "Deep learning framework for wireless systems: Applications to optical wireless communications." *IEEE Communications Magazine* 57.3 (2019): 35–41.
- [47] Lytvyn, Vasyl, et al. "Intelligent system of a smart house." *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*. IEEE, 2019.
- [48] Moslehi, Khosrow, and Ranjit Kumar. "A reliability perspective of the smart grid." *IEEE Transactions on Smart Grid* 1.1 (2010): 57–64.
- [49] Fang, Xi, et al. "Smart grid—The new and improved power grid: A survey." *IEEE Communications Surveys & Tutorials* 14.4 (2011): 944–980.
- [50] Al-Omari, Mohammad, et al. "An intelligent tree-based intrusion detection model for cyber security." *Journal of Network and Systems Management* 29 (2021): 1–18.
- [51] Azeez, Nureni Ayofe, et al. "Intrusion detection and prevention systems: An updated review." *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019 1* (2020): 685–696.
- [52] Kruegel, Christopher, and Thomas Toth. "Using decision trees to improve signature-based intrusion detection." In *Recent Advances in Intrusion Detection: 6th International Symposium, RAID 2003, Pittsburgh, PA, USA, September 8–10, 2003. Proceedings* 6. Springer, 2003.
- [53] Jyothsna, V. V. R. P. V., Rama Prasad, and K. Munivara Prasad. "A review of anomaly based intrusion detection systems." *International Journal of Computer Applications* 28.7 (2011): 26–35.
- [54] Alshehri, Fatima, and Ghulam Muhammad. "A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare." *IEEE Access* 9 (2020): 3660–3678.
- [55] Chen, Xieling, et al. "Information fusion and artificial intelligence for smart healthcare: A bibliometric study." *Information Processing & Management* 60.1 (2023): 103113.
- [56] Ragavi, B., et al. "Smart agriculture with AI sensor by using Agrobot." *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2020.
- [57] Qazi, Sameer, Bilal A. Khawaja, and Qazi U. Farooq. "IoT-equipped and AI-enabled next generation smart agriculture: A critical review, current challenges and future trends." *IEEE Access* 10 (2022): 21219–21235.
- [58] Choo, Kim-Kwang Raymond. "The cyber threat landscape: Challenges and future research directions." *Computers & Security* 30.8 (2011): 719–731.
- [59] Stevens, Tim. "Knowledge in the grey zone: AI and cybersecurity." *Digital War* 1 (2020): 164–170.
- [60] Wirkuttis, Nadine, and Hadas Klein. "Artificial intelligence in cybersecurity." *Cyber, Intelligence, and Security* 1.1 (2017): 103–119.

- [61] Repalle, Syam Akhil, and Venkata Ratnam Kolluru. "Intrusion detection system using ai and machine learning algorithm." *International Research Journal of Engineering and Technology (IRJET)* 4.12 (2017): 1709–1715.
- [62] Modi, Chirag, et al. "A survey of intrusion detection techniques in cloud." *Journal of Network and Computer Applications* 36.1 (2013): 42–57.
- [63] Chao-Yang, Zhang. "DOS attack analysis and study of new measures to prevent." *2011 International Conference on Intelligence Science and Information Engineering*. IEEE, 2011.
- [64] Douligeris, Christos, and Aikaterini Mitrokotsa. "DDoS attacks and defense mechanisms: Classification and state-of-the-art." *Computer Networks* 44.5 (2004): 643–666.
- [65] Bassil, Ramzi, et al. "Security analysis and solution for thwarting cache poisoning attacks in the domain name system." *2012 19th International Conference on Telecommunications (ICT)*. IEEE, 2012.
- [66] Levine, Brian Neil, Clay Shields, and N. Boris Margolin. *A Survey of Solutions to the Sybil Attack*. Technical Report of University of Massachusetts Amherst, Vol. 7 (2006): 224.
- [67] Yihunie, Fekadu, Eman Abdelfattah, and Ammar Odeh. "Analysis of ping of death DoS and DDoS attacks." *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*. IEEE, 2018.
- [68] Kussyk, Janusz, M. Umit Uyar, and Cem Safak Sahin. "Survey on evolutionary computation methods for cybersecurity of mobile ad hoc networks." *Evolutionary Intelligence* 10 (2018): 95–117.
- [69] Thakkar, Ankit, and Ritika Lohiya. "Role of swarm and evolutionary algorithms for intrusion detection system: A survey." *Swarm and Evolutionary Computation* 53 (2020): 100631.
- [70] Li, Jian-hua. "Cyber security meets artificial intelligence: A survey." *Frontiers of Information Technology & Electronic Engineering* 19.12 (2018): 1462–1474.

5 Cyber Threat Actors Review

Examining the Tactics and Motivations of Adversaries in the Cyber Landscape

Zakaria Abou El Houda

5.1 INTRODUCTION

In today's digital world, the threat of cyber attacks continues to grow. The increasing number of cyber incidents reported in recent years has highlighted the vulnerability of individuals, organizations, and nations to cyber threats. Cyber threat actors are becoming more sophisticated in their methods, and their attacks can have severe consequences for their victims. According to recent studies, about 80% of cyber security incidents involve phishing attacks, while email transmission accounts for 90% of malware. Additionally, ransomware attacks are increasingly common, and statistics show that they occur every 10 seconds globally. Such attacks use relatively simple software to shut down targeted company operations entirely, and shockingly, 32% of companies pay the ransom demands to recover their data, further enabling cyber criminal groups to operate like legitimate businesses. The purpose of this chapter is to examine the tactics and motivations of cyber threat actors in the current cyber landscape. The research aims to identify the different types of cyber threat actors, analyze their tactics, and understand their motivations. By doing so, we aim to provide recommendations for organizations and governments on how to counter the threats posed by cyber threat actors [1–9].

The digital age has brought about a new era of cyber threats that can cause significant harm to individuals, organizations, and even nations. Cyber threat actors are groups of individuals, organizations, or nation-states that use digital means to launch attacks against their targets. These attacks can range from stealing personal information to disrupting critical infrastructure. One of the biggest challenges in countering cyber threats is understanding the tactics used by cyber threat actors. These tactics can be broken down into several categories, including social engineering, malware, and ransomware. Social engineering tactics are used to manipulate individuals into divulging confidential information or providing access to restricted systems. Malware, on the other hand, is a software program that is designed to harm

computer systems, steal data, or control a system remotely. Ransomware is a type of malware that encrypts data on a victim's system and demands a ransom payment in exchange for the decryption key [10–34].

Understanding the motivations of cyber threat actors is also crucial in countering cyber threats. Some threat actors are motivated by financial gain, while others are motivated by espionage or political influence. Nation-state actors, for example, are often motivated by geopolitical interests and use cyber attacks to further their strategic objectives. Criminal organizations, on the other hand, are primarily motivated by financial gain and use cyber attacks to steal personal information or intellectual property. The different types of cyber threat actors can be categorized into nation-states, criminal organizations, and hacktivists. Nation-state actors are often the most sophisticated and well funded threat actors, with access to advanced tools and techniques. Criminal organizations, on the other hand, are often motivated by financial gain and use a range of tactics to achieve their objectives. Hacktivists are a type of cyber threat actor that are motivated by political or social causes and often launch attacks against governments or corporations. The risks posed by cyber threat actors are significant, and organizations and governments must take steps to protect themselves. Countermeasures can include risk management, cyber defense, and cyber resilience. Risk management involves identifying and assessing the risks posed by cyber threats and developing strategies to mitigate those risks. Cyber defense involves implementing measures to prevent, detect, and respond to cyber attacks. Cyber resilience involves preparing for and recovering from cyber incidents. The first objective of this research proposal is to identify the different types of cyber threat actors. This will involve categorizing cyber threat actors based on their motivation, tactics, and level of sophistication. The three main types of cyber threat actors are nation-states, criminal organizations, and hacktivists. The review will examine the characteristics of each type of cyber threat actor and the tactics they use to launch attacks. The second objective is to analyze the tactics used by cyber threat actors. The review will focus on the different tactics used by cyber threat actors, including social engineering, malware, and ransomware. The review will examine the different types of social engineering tactics used by cyber threat actors, such as phishing, pretexting, and baiting. Additionally, the review will analyze the various types of malware, including viruses, Trojans, and worms, and their respective impacts on computer systems. Finally, the review will analyze the use of ransomware, which has become a popular tactic used by cyber threat actors in recent years. The third objective is to examine the motivations of cyber threat actors. This review will analyze the different motivations behind cyber attacks, including financial gain, espionage, and political influence. The review will examine the different types of cyber attacks that are motivated by financial gain, including the theft of financial information and the use of ransomware. Additionally, the review will analyze the motivations of nation-state actors and hacktivists, who are often motivated by political or social causes. The fourth objective is to provide recommendations for organizations and governments on how to counter the threats posed by cyber threat actors. The recommendations will be based on the findings of the review and will focus on risk management, cyber defense, and cyber resilience. Risk management strategies will involve identifying and assessing the risks posed by cyber threats and developing strategies to mitigate

those risks. Cyber defense strategies will involve implementing measures to prevent, detect, and respond to cyber attacks. Cyber resilience strategies will involve preparing for and recovering from cyber incidents.

The main contributions of this chapter can be summarized as follows:

- We review the existing literature on cyber threat actors and their tactics and motivations.
- We identify the different types of cyber threat actors, including nation-states, criminal organizations, and hacktivists.
- We analyze the tactics used by cyber threat actors, including social engineering, malware, and ransomware.
- We examine the motivations of cyber threat actors, including financial gain, espionage, and political influence.
- We identify the different types of cyber threat actors, including nation-states, criminal organizations, and hacktivists.
- We provide recommendations for organizations and governments on how to counter the threats posed by cyber threat actors.

5.2 ACTORS

This section presents an overview of three important cyber threat actors: APT 29, Conti, and LAPSUS\$. The section highlights the differences in the scope of attack and methods used by each actor. APT 29 is described as primarily seeking to attack government organizations based in Europe and belonging to NATO, with a focus on sophisticated methods of penetration. Conti is said to focus on high-income companies, using zero-day vulnerabilities and double extortion to maximize their ransom collection and installing backdoors to resell turnkey access to malicious operators. LAPSUS\$, on the other hand, targets big tech companies such as Samsung and NVIDIA, using unsophisticated attacks to steal data and demand ransom for non-disclosure. The section concludes by emphasizing the importance of following best practices in cyber security, as the cyber menace continues to increase.

5.2.1 METHODOLOGY

The first step of our research consists of identifying the actors of the cyber threat landscape in 2022 by setting up a cyber security watch. Real-time alerts being the target, we went to Twitter. After jumping from account to account over a couple of weeks, we were able to create a diffusion list called Threat Intelligence. This list contains several CERT accounts, cyber security specialists, and companies specializing in Threat Intelligence. To make the link with this Twitter list, we subscribed to some RSS feeds. Those feeds from famous newspapers and specialists allow us to have more insights on the current threats. For example, we followed the CERT-FR, Schneier on Security, Krebs on Security, Security Week, and Hacker News. We especially analyzed the reports from Mandiant, Unit 42—Palo Alto Networks, CrowdStrike, Red Canary, IBM X-Force, Google Threat Analysis Group (TAG), Cisco Talos Intelligence Group, and Rapid [7].

Those companies provide cyber security services, which allow them to have insights into the current threats. As they are global companies, their threat reports allow us to have a deeper understanding of the current cyber threat landscape. We correlated the information gathered in the threat reports with the results of the first step, which allowed us to identify the most relevant threat actors in 2023.

5.2.2 TYPE OF THREAT ACTORS

Based on our research, the most relevant threat actors in the cyber threat landscape in 2023 are:

1. **Nation-State Actors:** Nation-state actors are government-sponsored cyber attackers who use sophisticated techniques to achieve their objectives. They are well-funded and have access to advanced tools and technologies, making them a significant threat to businesses and governments.
2. **Cyber Criminals:** Cyber criminals are individuals or groups who engage in illegal activities for financial gain. They use various techniques such as phishing, ransomware, and social engineering to target individuals and organizations.
3. **Hactivists:** Hactivists are individuals or groups who use hacking as a form of activism. They target organizations that they believe are engaging in unethical practices or violating human rights.
4. **Insiders:** Insiders are individuals within an organization who have access to sensitive information and use it for personal gain or to harm the organization. They can be employees, contractors, or partners.
5. **Advanced Persistent Threat (APT) Groups:** APT groups are well funded and organized cyber attackers who target specific organizations or industries over an extended period. They use sophisticated techniques such as zero-day exploits and advanced malware to achieve their objectives.

5.3 ACTORS PRESENTATION

In this section, we highlight some of the most active threat actors.

5.3.1 CONTI GANG

Conti is a type of ransomware that emerged in late 2019 and is believed to have originated from Ryuk, which was developed by the Russian hacker group Wizard Spider, known for creating various other malware such as TrickBot and Bazar-Loader. Conti has recently targeted companies such as SEA-Invest, Nordex, and the Costa Rican government, demanding high ransoms and causing damage to their reputations, severe fines related to GDPR law, and economic damage.

Conti ransomware is a sophisticated malware that has been linked to the Russian hacker group Wizard Spider. As previously mentioned, while there is no official confirmation of their involvement, leaked conversations between members of the group indicate close collaboration with the Russian government. This connection

suggests that the group may be working in the interests of the Russian state, using ransomware attacks to generate revenue and advance political goals. One of the key features of the Conti group is its organizational structure, which resembles that of a traditional company. The group has a human resources department, recruitment officers, and teams responsible for budgets, accounting, salaries, and other business functions. They also have a physical office located in St. Petersburg, which is in close proximity to the local branches of the FSB and the Ministry of the Interior, providing further evidence of a potential link to the Russian government.

Conti's strategy is based on the Big Hunt Gaming approach, which involves exploiting zero-day vulnerabilities and using manual, stealthy propagation techniques to remain undetected. Their targets are typically entities with high revenues or those whose business is vital, such as large corporations, critical infrastructure, and government institutions. The group uses a double extortion technique, which involves stealing data before encrypting it, thereby maximizing their chances of receiving the ransom. They then threaten to release the stolen information if the victim fails to pay. To maximize their profits, the group has a team dedicated to negotiation and OSINT (Open Source INTelligence). This team conducts extensive investigations to identify the most appropriate parties to pay, sets an acceptable amount for the victim, and determines the pressure tactics to be used in the negotiation phases. Conti has targeted a wide range of organizations, including SEA-Invest, Nordex, and the Costa Rican government. The attacks on SEA-Invest and Nordex illustrate the group's ability to target large, multinational corporations with sophisticated security systems, while the attack on the Costa Rican government highlights their willingness to target critical infrastructure and government institutions. The Conti group's activities have significant economic and political implications, as their attacks can cause serious financial and reputational damage to their victims. Furthermore, their links to the Russian government suggest that their activities may be part of a broader political agenda. As such, it is essential for organizations and governments to remain vigilant and take steps to mitigate the risk of Conti and other similar ransomware attacks. With its 1,000th victim recorded in March 2022, Conti has established itself as one of the most active groups in recent months. Among the most recent are SEA-Invest, one of the world's largest terminal operators for dry bulk, breakbulk, fruit, and liquid bulk, that is active in no fewer than 25 ports spread across two continents. The attack was claimed by the group on February 7, 2022. At the moment, a small portion of the data has been leaked on Conti's website, leading one to believe that the company is still in negotiations with its attackers. The attack came days after a cyber attack on Oiltanking, a German oil and gas transportation company. In addition to the financial interest of this sector, it can also be seen as a political action to destabilize the gas supply of European countries, in coordination with the Russian invasion of Ukraine. Another example is Nordex, one of the world's largest wind turbine developers and manufacturers, with more than 8,500 employees. The attack was identified on April 2, 2022, and the company's data is already accessible online. The full exposure of the company's data raises the question of the financial value of this attack. It is easy to imagine that the group was unable to obtain funding for its ransom. The hackers would have installed a persistent backdoor in the company's system in order to make CaaS (cyber crime as a service) by reselling turnkey access to malicious operators.

The latest and most recent example is the attack on the Costa Rican government. In April, the Conti group announced that it had impacted 27 government institutions and harvested more than 650 gigabytes of data. They are now demanding a ransom of \$20 million and are trying to arouse the people to force the government to pay. In order to do so, they have made the family allowance fund, the social security system, the meteorological agency, and the inter-university systems unavailable.

5.3.2 LAPSUS

LAPSUS\$ is a notorious hacker group that has targeted various large tech companies, including Microsoft, Nvidia, and Samsung. The group's activities began in December 2021 with a breach in the Brazilian Health Ministry's computer systems, and it has since expanded its targets to entities in the telecommunications and gaming sectors, call centers, and server hosts. The group claims to be apolitical and not affiliated with any state.

One of LAPSUS\$'s main strengths is its ability to recruit "insiders" to obtain valid credentials and gain legitimate access to companies' networks. The group carries out the initial compromise of information systems with the help of malicious collaborators who sell VPN, RDP, or CITRIX access in exchange for money. The recruitment of these insiders is done on two Telegram channels: LAPSUS\$ and LAPSUS\$ chat, both of which are publicly available.

Once inside a network, LAPSUS\$ typically exfiltrates data before threatening to publish it or making other demands, such as ransom demands or product modifications. The group's attacks and demands vary from victim to victim, and its operators have created new virtual machines in a target's cloud environment to conduct subsequent attacks.

LAPSUS\$ uses various techniques to gain initial access, including the deployment of the Redline Stealer malware and buying valid credentials from Dark Web forums or paying collaborators or suppliers to gain access to legitimate credentials. Once inside the system, the group typically exploits critical vulnerabilities to elevate their privileges and shape the victim's environment to suit their purposes.

Although the operators of LAPSUS\$ appear to be unprofessional and limited in number, the group's ability to compromise other networks in the future is expected to remain high due to the recruitment of insiders. Future releases of compromised data can be expected in the coming weeks.

5.3.3 APT29

APT29, also known as Cozy Bear, has been active since at least 2008 and is believed to be associated with the Russian Federation's Foreign Intelligence Service (SVR) according to the U.S. and UK governments.

APT29 primarily targets government networks in European and NATO countries, as well as research institutes, pharmaceutical companies, and consulting firms. This group is known for using sophisticated techniques with homegrown malware, such as stealing session cookies to bypass multifactor authentication and carrying out supply chain attacks.

One notable attack carried out by APT29 was against SolarWinds in 2020. The group compromised the update system of SolarWinds' Orion software, which allowed them to access the data of organizations using the software. This attack affected 18,000 companies or institutions, including American and foreign institutions.

APT29 has also targeted organizations involved in the development of the COVID-19 vaccine in the United States, Canada, and the UK, presumably to steal information and intellectual property related to the development of the vaccine. The group uses recently published CVE vulnerabilities to gain initial access into the system and then uses their in-house malware called WellMess and Well-Mail to execute commands or scripts. They also use spear-phishing to obtain web portal authentication information.

It is important for organizations to be aware of APT29's tactics and take appropriate measures to protect their networks and sensitive information from such attacks.

5.3.4 COMPARATIVE ANALYSIS OF APT 29, CONTI, AND LAPSUS\$

APT 29, Conti, and LAPSUS\$ are three important cyber threat actors. While the first two are unofficially affiliated with the Russian government, LAPSUS\$ claims to be completely independent of any state group. The scope of attack also differs among the three actors.

APT 29 primarily seeks to attack government organizations based in Europe and belonging to NATO. Conti focuses on hunt big game companies, high-income companies whose business is vital. LAPSUS\$ targets big tech companies such as Samsung and NVIDIA. LAPSUS\$ conducts large but unsophisticated attacks. They buy initial access on the darknet, using previously identified vulnerabilities to steal data and demand a ransom for their non-disclosure.

Conti works similarly to a state-run group, using zero-day vulnerabilities and seeking to discreetly propagate themselves on their victim's IS. They then use double extortion to maximize their chances of collecting the ransom and also install backdoors to resell turnkey access to malicious operators.

Finally, APT 29 uses much more sophisticated methods to penetrate highly protected systems and to reach a maximum number of strategic points. Their objective is more related to espionage and destabilization than to profit, even if part of their activities are dedicated to profit.

5.3.5 AI CYBER THREAT ACTORS

AI cyber threat actors are a growing concern in the cyber security landscape. As artificial intelligence (AI) technology advances, both defenders and attackers are leveraging it for their purposes. Let's review some common AI cyber threat actors, their tactics, and motivations:

- **AI-Powered Malware:** Adversaries are increasingly incorporating AI techniques into malware to evade detection and improve attack effectiveness. AI-powered malware can automatically adapt its behavior, obfuscate

malicious code, and exploit vulnerabilities in real time. These threats use machine learning algorithms to study defensive measures and develop evasion tactics. The motivation behind AI-powered malware is often financial gain through activities such as data theft, ransomware attacks, or cryptocurrency mining.

- **AI-Driven Social Engineering:** AI can be employed to enhance social engineering attacks. Threat actors use AI algorithms to analyze large datasets and create sophisticated phishing emails, messages, or voice recordings that mimic trusted individuals or organizations. These AI-driven attacks aim to deceive victims into revealing sensitive information, granting unauthorized access, or downloading malware. Motivations behind AI-driven social engineering attacks are typically focused on financial gain, unauthorized access to systems, or stealing valuable data.
- **AI-Enabled Botnets:** Botnets, networks of compromised computers controlled by a central entity, are being enhanced with AI capabilities. AI-enabled botnets leverage machine learning algorithms to improve their evasion techniques, automate attacks, and increase their efficiency. These botnets can launch distributed denial-of-service (DDoS) attacks, distribute malware, or spam campaigns. The motivations behind AI-enabled botnets vary, including financial gain through renting botnets, disrupting services, or conducting large-scale cyber attacks.
- **Adversarial Machine Learning:** Adversarial machine learning involves manipulating AI systems to deceive or bypass their defenses. Attackers can craft adversarial examples—subtle modifications to input data—that can fool AI algorithms, leading to misclassifications or incorrect decisions. Adversarial machine learning techniques can be employed to evade intrusion detection systems, bypass biometric authentication, or manipulate AI-powered decision-making processes. Motivations behind adversarial machine learning attacks can include causing disruptions, undermining AI-based security measures, or gaining unauthorized access.
- **AI-Augmented Advanced Persistent Threats (APTs):** APT groups are utilizing AI techniques to enhance their attack capabilities. They employ AI for reconnaissance, automating attack processes, optimizing malware payloads, or conducting targeted attacks with improved evasion techniques. AI-augmented APTs often have significant resources, including access to advanced AI technologies. Their motivations can range from espionage and intellectual property theft to gaining strategic advantages or disrupting critical infrastructure.

It's important to note that AI is a double-edged sword in cyber security, as defenders can also leverage AI for threat detection, anomaly detection, and behavior analysis to enhance their security measures. As AI technologies continue to advance, both defenders and threat actors will likely rely on AI-driven techniques in an ongoing arms race in the cyber landscape. Staying up-to-date with AI cyber security advancements and adopting appropriate defensive strategies is crucial to mitigate the risks associated with AI cyber threats [35–41].

5.3.6 BLOCKCHAIN CYBER THREAT ACTORS

When it comes to the blockchain ecosystem, specific threat actors target this technology. Let's review some of these actors, their tactics, and motivations:

- **Cryptojackers:** Cryptojackers are cyber criminals who exploit vulnerabilities in blockchain networks or web applications to mine cryptocurrencies without the owner's consent. They typically target public blockchains or decentralized applications (DApps). Their primary motivation is financial gain through the illicit mining of cryptocurrencies. Cryptojackers often employ tactics like injecting malicious scripts into websites, spreading malware through phishing emails, or compromising vulnerable servers.
- **Smart Contract Exploiters:** Smart contract exploiters focus on finding vulnerabilities or coding errors in smart contracts deployed on blockchain platforms. They exploit these weaknesses to manipulate the intended behavior of smart contracts, leading to unauthorized access, fund theft, or other malicious activities. Their motivations include stealing funds, disrupting blockchain applications, or causing reputational damage. These actors may employ techniques like reentrancy attacks, integer overflow/underflow, or front-running attacks to exploit smart contracts.
- **51% Attackers:** In blockchain networks that rely on consensus algorithms like Proof of Work (PoW), 51% attackers aim to control the majority of the network's computational power. By doing so, they can manipulate the blockchain's transaction history, double-spend cryptocurrencies, or exclude legitimate transactions from being confirmed. The motivation behind 51% attacks varies, ranging from financial gain to causing disruption or damaging the reputation of a particular blockchain network.
- **Social Engineers:** Social engineers target individuals within the blockchain ecosystem to exploit human vulnerabilities. They employ techniques such as phishing, impersonation, or social media manipulation to deceive victims into revealing private keys, sensitive information, or granting unauthorized access to blockchain accounts. Motivations for social engineering attacks can include stealing funds, gaining control over blockchain wallets, or conducting identity theft.
- **State-Sponsored Actors:** Similar to the threats faced by the broader cyber security landscape, state-sponsored threat actors may also target blockchain technology. Their motivations can range from gaining economic advantages through intellectual property theft or disrupting blockchain-based systems for political reasons. State-sponsored actors may employ advanced techniques, including zero-day exploits, supply chain attacks, or targeted phishing campaigns, to compromise blockchain networks or steal sensitive data. It's important to note that these threat actors and their tactics are constantly evolving as blockchain technology matures. Consequently, it's crucial to stay informed about emerging threats and to adopt appropriate security measures to mitigate risks in the blockchain ecosystem.

5.4 DEFENSIVE TECHNIQUES AND ADAPTATIONS

Defensive techniques and adaptations refer to strategies and measures that individuals and organizations can implement to protect themselves against cyber threats. With the increasing frequency and sophistication of cyber attacks, it is critical for individuals and organizations to adopt proactive measures to safeguard their digital assets and data.

One of the most effective defensive techniques is to regularly update software and applications to ensure that known vulnerabilities are patched. This includes operating systems, web browsers, and other software programs that are used frequently. Another effective technique is to use strong and unique passwords for all accounts and to enable two-factor authentication wherever possible.

Additionally, individuals and organizations should implement network segmentation and access controls to limit the potential impact of a cyber attack. This involves dividing a network into smaller, more manageable segments and limiting access to sensitive information only to authorized personnel. Data backups should also be performed regularly, with backups stored in secure and separate locations to prevent the loss of critical data in the event of a cyber attack.

5.4.1 IoC AND BEHAVIOR ANALYSIS WITH UEBA

Indicators of compromise (IoCs) are pieces of information that provide evidence of a cyber attack, such as IP addresses, domain names, file hashes, and other characteristics of malicious activity. IoCs can be used to detect and respond to attacks and to prevent future incidents by identifying patterns and trends.

Behavior analysis is another important tool for cyber security, as it can help detect abnormal or suspicious activity that might indicate an attack. User and entity behavior analytics (UEBA) is a type of behavior analysis that focuses on identifying unusual patterns of behavior among users and other entities in a network. UEBA uses machine learning algorithms to analyze data from a variety of sources, including logs, network traffic, and other security data.

One way to use IoCs and behavior analysis together is to use IoCs as input to UEBA algorithms. For example, IoCs can be used to train a UEBA model to recognize known patterns of attack and to flag suspicious behavior that might indicate a new or unknown threat. UEBA can also be used to correlate IoCs with other types of security data, such as logs and network traffic, to provide a more complete picture of an attack and its impact on the network.

Mathematically, UEBA algorithms can be represented as follows:

Let X be the set of input features, such as user behavior, network traffic, and other security data. Let y be the output variable, representing whether a given entity is exhibiting normal or abnormal behavior. UEBA algorithms seek to learn a function $f(X) = y$ that maps the input features to the output variable, using techniques such as supervised learning, unsupervised learning, and reinforcement learning.

UEBA algorithms can also incorporate IoCs into the learning process by adding IoCs as additional input features. For example, an algorithm might include IP addresses, domain names, or other indicators of compromise as features in a

machine-learning model. The model can then use these features to learn patterns of attack and to flag suspicious behavior that might indicate a new or unknown threat.

In summary, IoCs and behavior analysis with UEBA are important tools for detecting and responding to cyber attacks. By incorporating IoCs into UEBA algorithms, security professionals can gain a more complete picture of an attack and its impact on the network and can respond more quickly and effectively to protect against future incidents.

It is estimated that one user produces about 25,000 logs each day, so there is a need to automate the task. To do this, a SIEM (security information and event management) can be used. This collects the logs of the various services of an information system, analyzes them in order to detect malicious actions, and finally issues alerts. However, it is necessary to create detection rules beforehand in order to receive alerts.

Unfortunately, IoC detection is reactive in nature; i.e., when one is found, it is often too late, and the system has probably already been compromised. Nevertheless, this considerably reduces the time of detection and allows the necessary measures to be taken as quickly as possible in order to limit the propagation or even stop the attack.

5.4.1.1 Risk Assessment Model

$$\text{Risk} = \text{Probability} \times \text{Impact} \quad (5.1)$$

where Risk is the overall level of risk, Probability is the likelihood of a threat occurring, and Impact is the potential damage that could result from the threat.

5.4.1.2 Attack Surface Model

$$\text{Attack Surface} = \sum_{i=1}^n A_i \quad (5.2)$$

where Attack Surface is the total area or number of entry points that an attacker can exploit, and A is the number of entry points or attack vectors.

5.4.1.3 Intrusion Detection Model

$$\text{Detection Rate} = \frac{TP}{TP + FN} \quad (5.3)$$

where Detection Rate is the proportion of true positive detections, TP is the number of true positive detections, and FN is the number of false negative detections.

5.4.1.4 Defense-in-Depth Model

$$\text{Security Level} = \sum_{i=1}^n L_i \quad (5.4)$$

where Security Level is the overall level of security, L is the level of security for each layer or component, and n is the number of layers or components.

5.4.1.5 Game Theory Model

$$\text{Payoff}_A = \begin{cases} R, & \text{if A cooperates and B cooperates } S \\ \text{if A cooperates and B defects } T, & \text{if A defects and B cooperates } P \\ \text{if A defects and B defects} & \end{cases} \quad (5.5)$$

where Payoff is the reward or penalty for a player, R is the reward for mutual cooperation, S is the penalty for being exploited, T is the temptation to defect, and P is the punishment for mutual defection. This model can be used to analyze the behavior of attackers and defenders in a cyber security scenario:

- Unusual outgoing and incoming network traffic
- Geographical irregularity: Traffic or attempted connections from areas or countries where the organization is not present
- Unusual user account activity: User attempting to elevate privileges or access an account with higher privileges
- Increase in the volume of a database read: When exfiltrating data, suspicious changes to the registry or system files
- Anomalies in DNS queries: For example, when a command and control (CC) server sends commands
- An increase in incorrect connections, which may indicate brute force attacks

As previously explained, it is necessary to have already identified indicators of compromise and to create rules, so that they can be automatically detected later. Thus UEBA (user and entity behavior analytics) allows the detection of unknown threats, especially internal ones. Thanks to machine learning, it is possible to create a reference for “normal” behavior of a user, a group, or a network entity. Then, when the user performs a new action that deviates from the expected behavior, an alert with a risk score is automatically raised.

5.4.2 ARTIFICIAL INTELLIGENCE (AI)

Artificial Intelligence (AI) has the potential to significantly enhance an organization’s ability to mitigate cyber threats by automating threat detection and response and by providing faster and more accurate insights into potential security breaches. Here are a few ways that AI can be used to mitigate cyber threats:

- **Threat Detection:** AI can be used to analyze vast amounts of data to identify patterns and anomalies that could indicate a security breach. Machine learning algorithms can be trained on historical data to detect and respond to new types of threats in real time. This can help organizations to identify and respond to threats faster, reducing the time that attackers have to cause damage.
- **Network Security:** AI can be used to monitor network traffic in real time to identify potential threats, such as unauthorized access attempts, suspicious

activity, or data exfiltration. AI-powered intrusion detection systems (IDS) can automatically identify and block malicious traffic, reducing the risk of a successful cyber attack.

- **Fraud Detection:** AI can be used to detect fraudulent activity, such as payment fraud, identity theft, or account takeover. Machine learning algorithms can analyze transactional data to identify patterns of behavior that are indicative of fraud and can alert security teams to take action.
- **Incident Response:** AI can be used to automate incident response processes, such as isolating infected systems, quarantining suspicious files, or blocking malicious IP addresses. This can help organizations to respond faster to security incidents, minimizing the impact of a cyber attack.
- **Predictive Analytics:** AI can be used to predict potential cyber threats by analyzing historical data and identifying patterns that are indicative of an attack. This can help organizations to take proactive measures to prevent a cyber attack before it happens, such as by patching vulnerabilities, strengthening access controls, or enhancing security awareness training.
- **User Behavior Analytics:** AI can be used to analyze user behavior to identify potential insider threats. Machine learning algorithms can learn typical user behavior patterns and can detect when users are behaving abnormally or accessing data that they shouldn't be. This can help organizations to detect and respond to insider threats more quickly, reducing the risk of data loss or theft.
- **Natural Language Processing:** AI can be used to analyze text data, such as emails or chat messages, to identify potential security threats. Natural language processing (NLP) algorithms can detect suspicious language, such as requests for sensitive information, or phishing attempts. This can help organizations detect and respond to social engineering attacks more effectively.
- **Threat Intelligence:** AI can be used to analyze threat intelligence feeds to identify emerging cyber threats. Machine learning algorithms can learn from historical threat data and can predict the likelihood of a new threat being successful. This can help organizations to prioritize their security measures and allocate resources more effectively.

5.4.3 ZERO-TOUCH AND ZERO-TRUST SYSTEM SECURITY MODELS

Zero-touch and zero-trust are two security frameworks that can help organizations defend against the evolving cyber threats posed by AI adversaries. Let's explore how these frameworks can be leveraged to enhance security:

5.4.3.1 Zero-Touch

Zero-touch focuses on automating security processes to minimize human intervention and reduce the attack surface. In the context of AI cyber threats, zero-touch can be implemented through the following measures:

1. **Automated Threat Detection:** Utilize AI-powered security solutions to automatically detect and respond to AI-driven attacks. These solutions can

analyze network traffic, behavior patterns, and anomalous activities to identify potential threats.

2. **Continuous Monitoring:** Implement real-time monitoring mechanisms that leverage AI for anomaly detection. By continuously monitoring network traffic, system logs, and user behaviors, organizations can identify and respond to AI-based threats in a timely manner.
3. **Rapid Patching and Updates:** Automate the process of applying security patches and updates to minimize vulnerabilities. This helps prevent adversaries from exploiting known weaknesses in AI systems or other software components.
4. **Secure DevOps:** Incorporate security into the development and deployment processes of AI applications. Adopting DevSecOps practices ensures that security measures are implemented throughout the entire software development life cycle.

5.4.3.2 Zero-Trust

Zero-trust is a security framework that assumes no implicit trust, regardless of whether the user is inside or outside the network perimeter. It enforces strict access controls and continuously verifies and validates all devices, users, and applications before granting access. To defend against AI adversaries, zero-trust principles can be implemented as follows:

1. **Identity and Access Management (IAM):** Implement strong authentication mechanisms such as multifactor authentication (MFA) and biometrics to ensure that only authorized users can access sensitive systems or data. Additionally, adopt granular access controls and least privilege principles to limit user access to only what is necessary.
2. **Microsegmentation:** Divide the network into smaller, isolated segments using network segmentation techniques. This helps contain potential breaches and prevents lateral movement by adversaries within the network.
3. **Behavioral Analytics:** Employ AI-based behavioral analytics solutions that can detect anomalous user behaviors or deviations from established patterns. This helps identify compromised accounts, insider threats, or AI-driven attacks that exhibit unusual behaviors.
4. **Encryption and Data Protection:** Apply end-to-end encryption for sensitive data in transit and at rest. This ensures that even if adversaries gain access to encrypted data, they cannot exploit it without the decryption keys.
5. **Continuous Monitoring and Risk Assessment:** Implement continuous monitoring of network, user, and application activities to detect any potential security risks. Conduct regular risk assessments and vulnerability scans to identify and address any weaknesses in the AI infrastructure.

By combining the principles of zero-touch and zero-trust, organizations can establish a robust security posture against AI cyber threats. However, it's important to remember that security is an ongoing effort that requires regular updates, employee training, and staying informed about emerging threats and security best practices.

5.4.4 SECURITY MANAGEMENT

The preceding solutions can be quite complex and expensive to implement for small businesses; however, there are solutions that are quite simple and accessible to all. For example, we can follow the recommendations of various organizations such as ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) or ASD (Australia's Signals Directorate). Here are some examples: (1) Use a white list of applications to prevent the execution of malware, scripts, etc.; (2) apply the latest patches for applications such as Java, Web browser, and Microsoft Office; (3) keep your operating system up-to-date; and (4) Use multifactor authentication to connect to VPN, SSH, or any remote access.

To ensure that these recommendations are properly implemented within an organization, it is important to create a PSSI (information system security policy), which is a document containing the security rules that govern the company's information system. This is an integral part of an ISMS (information security management system), which provides a framework for how security is managed globally in the company. In particular, it addresses the three principles of information security: confidentiality, integrity, and availability.

Finally, the implementation of an ISMS is based on ISO standards, such as ISO27001, which defines the requirements.

5.5 CONCLUSION

In our analysis, we aimed to present the current cyber security landscape. We presented different types of threat actors to explain how each one works. In the future, the ransomware threat will probably continue its upward trend. The business of ransomware is simply too lucrative unless international governments and technology innovations can fundamentally alter the attacker's cost-benefit calculation.

While there have been efforts to disrupt operations and hold threat actors accountable, cyber criminals simply sign up with another platform—as part of the ransomware-as-a-service business model—to continue their operations. Nation-state actors will continue to organize attacks to serve their geopolitical interests. Above all, with the Ukrainian war, Russia has maintained an aggressive posture throughout 2022 and into 2023, with a sustained emphasis on targeting NATO, Eastern Europe, Ukraine, Afghanistan, and the energy sector.

As the business of ransomware is not going anywhere, and neither are espionage and information operations, new solutions exist to protect yourself or your organization. Therefore, following best practices in cyber security is more necessary than ever as the cyber menace continues to increase.

REFERENCES

1. S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 623–654, First quarter 2016.
2. Z. A. El Houda, L. Khoukhi, and A. Hafid, "Chainsecure—a scalable and proactive solution for protecting blockchain applications using SDN," in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, IEEE, Abu Dhabi, UAE, pp. 1–6.

3. D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Communications Surveys Tutorials*, vol. 19, no. 1, pp. 325–346, Firstquarter 2017.
4. Z. A. El Houda, A. Hafid, and L. Khoukhi, "Co-IoT: A collaborative DDoS mitigation scheme in IoT environment based on blockchain using SDN," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, IEEE, Waikoloa, HI, USA, pp. 1–6.
5. D. Zhou, Z. Yan, G. Liu, and M. Atiquzzaman, "An adaptive network data collection system in SDN," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 2, pp. 562–574, 2020.
6. Z. Abou El Houda, A. S. Hafid, and L. Khoukhi, "Cochain-sc: An intra- and inter-domain DDoS mitigation scheme based on blockchain using SDN and smart contract," *IEEE Access*, vol. 7, pp. 98 893–98 907, 2019.
7. Z. A. E. Houda, A. Hafid, and L. Khoukhi, "Blockchain meets AMI: Towards secure advanced metering infrastructures," in *ICC 2020–2020 IEEE International Conference on Communications (ICC)*, 2020, IEEE, Virtual Conference, pp. 1–6.
8. T. Alharbi, "Deployment of blockchain technology in software defined networks: A survey," *IEEE Access*, vol. 8, pp. 9146–9156, 2020.
9. Z. A. E. Houda, A. Hafid, and L. Khoukhi, "Blockchain-based reverse auction for v2v charging in smart grid environment," in *ICC 2021–2021 IEEE International Conference on Communications (ICC)*, 2021, IEEE, Virtual / Montreal, Canada, pp. 1–6.
10. H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT blockchain architecture using oracles and smart contracts: The use-case of a food supply chain," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, IEEE, Istanbul, Turkey, pp. 1–6.
11. H. Moudoud, L. Khoukhi, and S. Cherkaoui, "Prediction and detection of FDIA and DDoS attacks in 5g enabled IoT," *IEEE Network*, pp. 1–8, 2020.
12. H. Moudoud, S. Cherkaoui, and L. Khoukhi, "Towards a scalable and trustworthy blockchain: IoT use case," in *ICC 2021–2021 IEEE International Conference on Communications (ICC)*, 2021, pp. 1–6.
13. H. Moudoud, Z. Mlika, L. Khoukhi, and S. Cherkaoui, "Detection and prediction of FDI attacks in IoT systems via hidden Markov model," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 2978–2990, 2022.
14. H. Moudoud, S. Cherkaoui, and L. Khoukhi, "Towards a secure and reliable federated learning using blockchain," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 01–06.
15. H. Moudoud and S. Cherkaoui, "Toward secure and private federated learning for IoT using blockchain," in *GLOBECOM 2022–2022 IEEE Global Communications Conference*, 2022, IEEE, Rio de Janeiro, Brazil, pp. 4316–4321.
16. H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An overview of blockchain and 5g networks," *Computational Intelligence in Recent Communication Networks*, pp. 1–20, 2021.
17. F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.
18. Z. A. E. Houda, B. Brik, and L. Khoukhi, "'Why should I trust your IDS?': An explainable deep learning framework for intrusion detection systems in internet of things networks," *IEEE Open Journal of the Communications Society*, vol. 3, pp. 1164–1176, 2022.
19. Z. A. E. Houda, B. Brik, A. Ksentini, L. Khoukhi, and M. Guizani, "When federated learning meets game theory: A cooperative framework to secure IoT applications on edge computing," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7988–7997, 2022.

20. Z. A. El Houda, A. S. Hafid, and L. Khoukhi, "A novel machine learning framework for advanced attack detection using SDN," in *2021 IEEE Global Communications Conference (GLOBECOM)*, 2021, IEEE, Madrid, Spain, pp. 1–6.
21. Z. A. E. Houda, A. S. Hafid, and L. Khoukhi, "Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain," *IEEE Transactions on Network Science and Engineering*, pp. 1–17, 2023.
22. Z. A. El Houda, L. Khoukhi, and B. Brik, "A low-latency fog-based framework to secure IoT applications using collaborative federated learning," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022, IEEE, Edmonton, Canada, pp. 343–346.
23. Z. Abou El Houda, "Reinforcement de la sécurité' travers les réseaux programmables," Ph.D. dissertation, Universitéde Montréal, 2021.
24. Z. Abou El Houda, "Security enforcement through software defined networks (SDN)," Ph.D. dissertation, Troyes, 2021.
25. Z. Abou El Houda, A. Senhaji Hafid, and L. Khoukhi, *A Novel Unsupervised Learning Method for Intrusion Detection in Software-Defined Networks*. Cham: Springer International Publishing, 2022, pp. 103–117.
26. Z. Abou El Houda, A. S. Hafid, L. Khoukhi, and B. Brik, "When collaborative federated learning meets blockchain to preserve privacy in healthcare," *IEEE Transactions on Network Science and Engineering*, pp. 1–11, 2022.
27. Z. A. El Houda, L. Khoukhi, and A. S. Hafid, "Bringing intelligence to software defined networks: Mitigating DDoS attacks," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2020.
28. Z. Abou El Houda, S. Zerkane, D. Espes, and C.-T. Phan, "Method for processing a data packet and associated device, switching equipment and computer program," *Patent WO2 020 020 911A1*, January 2020. [Online]. Available: <https://hal.archives-ouvertes.fr/hal-03720399>
29. Z. A. El Houda, B. Brik, and S.-M. Senouci, "A novel IoT-based explainable deep learning framework for intrusion detection systems," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 20–23, 2022.
30. Z. Abou El Houda and L. Khoukhi, "A hierarchical fog computing framework for network attack detection in SDN," in *ICC 2022—IEEE International Conference on Communications*, 2022, IEEE, Seoul, South Korea, pp. 4366–4371.
31. Z. A. El Houda, B. Brik, A. Ksentini, and L. Khoukhi, "A mec-based architecture to secure IoT applications using federated deep learning," *IEEE Internet of Things Magazine*, vol. 6, no. 1, pp. 60–63, 2023.
32. Z. A. El Houda, B. Brik, and L. Khoukhi, "Ensemble learning for intrusion detection in SDN-based zero touch smart grid systems," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*, 2022, IEEE, Edmonton, Canada, pp. 149–156.
33. D. Adesina, C.-C. Hsieh, Y. E. Sagduyu, and L. Qian, "Adversarial machine learning in wireless communications using RF data: A review," *IEEE Communications Surveys Tutorials*, vol. 25, no. 1, pp. 77–100, 2023.
34. M. Ul Hassan, M. H. Rehmani, and J. Chen, "Anomaly detection in blockchain networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 25, no. 1, pp. 289–318, 2023.
35. "IEEE standard for criteria for security systems for nuclear power generating stations," *IEEE Std 692–2013* (Revision of IEEE Std 692–2010), pp. 1–57, 2013. [Online]. Available: <https://standards.ieee.org/ieee/692/5575/>
36. "IEEE guide for animal mitigation for electric power supply substations," *IEEE Std 1264–2022* (Revision of IEEE Std 1264–2015), pp. 1–48, 2022. [Online]. Available: <https://standards.ieee.org/ieee/1264/10562/>

37. H. Jo and K. Kim, "Security service-aware reinforcement learning for efficient network service provisioning," in *2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 2022, IEEE, Takamatsu, Japan, pp. 1–4.
38. P. Tague, D. Slater, J. Rogers, and R. Poovendran, "Evaluating the vulnerability of network traffic using joint security and routing analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 6, no. 2, pp. 111–123, 2009.
39. M. Sheng, H. Liu, X. Yang, W. Wang, J. Huang, and B. Wang, "Network security situation prediction in software defined networking data plane," in *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, 2020, IEEE, Dalian, Liaoning, China, pp. 475–479.
40. Fang Lan, W. Chunlei, Miao Qing, and Liu Li, "Dynamically validate network security based on adaptive control theory," in *2013 International Conference on Information and Network Security (ICINS 2013)*, 2013, IEEE, Bangkok, Thailand, pp. 1–6.
41. "IEEE standard for local and metropolitan area networks—media access control (mac) security corrigendum 1: Tag control information figure," *IEEE Std 802.1AE2018/Cor 1–2020* (Corrigendum to IEEE Std 802.1AE-2018), pp. 1–14, 2020. [Online]. Available: https://standards.ieee.org/ieee/802.1AE-2018_Cor_1/7588/

6 Layer-Based Security Threats in IoT Networks

Muna Muhammad, Ahthasham Sajid, and Hira Arshad

6.1 INTRODUCTION

The IoT is an inter-networking of things such as sensors, actuators, smart devices, intelligent systems, or anything consisting of transducers embedded in or connected via the Internet for sending and receiving data related to a particular application or service. The prevailing IoT applications usually provide high efficiency, automation, and comfort, as industries are currently producing a large number of IoT devices containing intelligent applications. The IoT has downgraded individual controlling and monitoring of services by providing smart services through smart applications such as smart home [1], smart farming [2], smart city [3], smart grids [4], smart manufacturing [5], etc. The extreme increase in IoT devices and services has embraced the whole world. Specifically, the entire world started to implement industrial revolutions and is bringing industries to the advanced level of the digital economy. Such applications are being supported by the operators using existing network and communication technologies. According to the *Global IoT Forecast Report 2021–30*, active IoT devices totaled 11.3 billion at the end of 2021, but this will dramatically increase to 29.4 billion by 2030 [6].

6.1.1 SECURITY IN THE IOT

With the huge number of IoT devices to be used in such a vast number of IoT applications [6], the communication between them needs to be secured so that user data is kept private, no attacks can occur in the IoT network, and no vulnerabilities are present. But, in general, IoT applications predictably face many security challenges because the smart devices in IoT network consume more power in terms of computation, high bandwidth, unsafe infrastructure, and open vulnerabilities. Without having a trusted and interoperable ecosystem of the IoT, its applications would not be able to fulfill the high demands and, due to this, might lose their potential [7]. Researchers have proposed different solutions for securing data exchange in IoT. IPV6 CoAP are the protocols proposed by [8] in order to secure networks in IoT, specifically the interoperability of the device. Along with the general security challenges faced by the Internet, WSNs, cellular networks, cloud computing, IoT also has its specific security challenges that still need to be solved, such as privacy data leakage, user authentication, user authorization, encryption, web interfaces, security threats, data storage, and so on.

TABLE 6.1
Factors Affecting Security of IoT and IT

IT Security	IoT Security
Extensive IT consists of many devices, and that is rich in resources.	Devices in IoT are required to be carefully provided with security measures, and that is poor in resources.
Widespread IT is dependent on devices that are rich in resources.	IoT systems consist of devices that are poor in terms of resources, such as software and hardware.
For wide security, complex algorithms are used.	Lightweight algorithms are preferred.
Has high security because of homogeneous technology.	IoT includes heterogeneous technology, due to which heterogeneous data is produced in high amounts, widening the attack surface.

Securing the IoT environment is usually more challenging than for general IT devices due to the many factors shown in Table 6.1 [7].

Given such vulnerabilities and issues, IoT environments pave the way for many cyber threats. The threats or attacks can occur in different layers of IoT networks; the general layers of the architecture of an IoT network are shown in Figure 6.1.

Because of the numerous security challenges in IoT applications, different solutions and techniques are needed in the same study in order to understand and secure the different IoT applications with different techniques. Hence this survey contains the following major contributions:

- Identifying security attacks in different layers of IoT networks
- Identifying security requirements in the Internet of Things applications or systems
- Classifying vulnerabilities, security threats, and open issues in IoT
- Review of current existing techniques and approaches for securing IoT systems
- Future research directions in IoT security

6.1.2 SECURITY CHALLENGES IN IOT

The ecosystem of the IoT is made up of integrating heterogeneous networks. This not only brings the generic problems of security from earlier communication networks, indeed it involves newer security problems by its specific properties. This starts with the sensor devices and includes monitoring the environmental variables and being responsible for the merging of virtual and physical worlds in IoT. The sensor devices pose limited storage and computing capacities, preventing complex and robust security systems, such as for authentication purposes [9]. Another aspect is the heterogeneity of IoT devices’ potential mobility and pervasiveness. As any physical device or object can be installed and becomes part of the IoT, the attack surface greatly increases. Smart environments’ connecting in IoT networks pose different

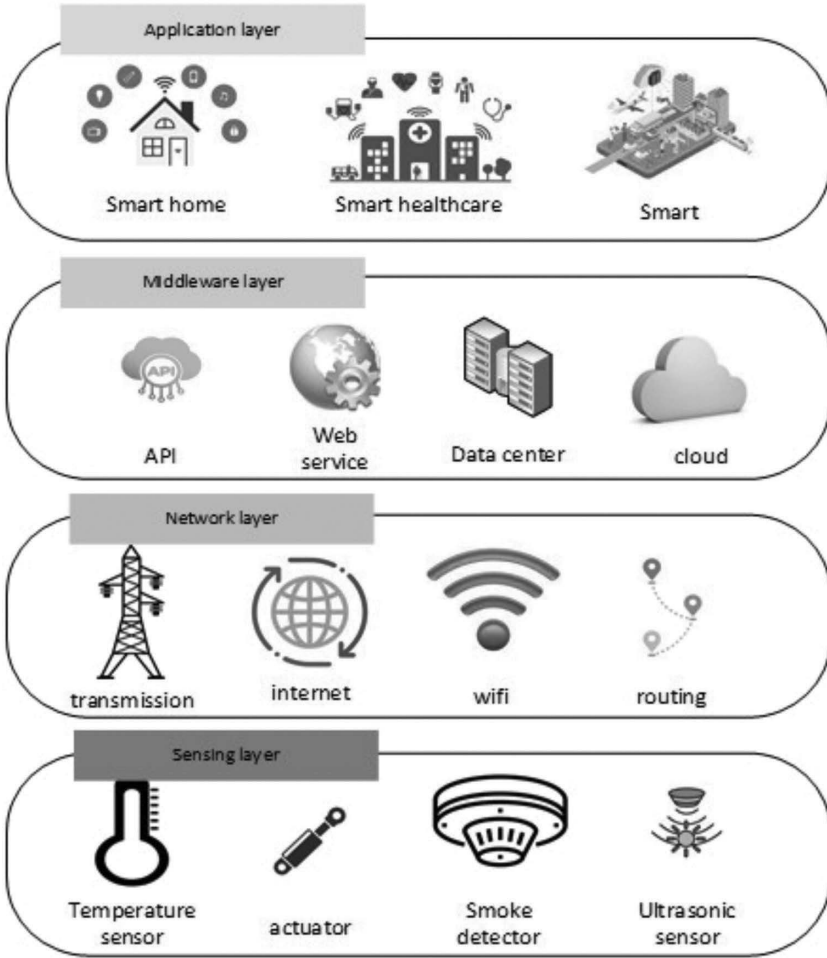


FIGURE 6.1 Layer-based issues and attacks in IoT.

vulnerabilities, which can be exploited by attackers. Along with that, for the access control and the authentication processes, it is tougher to manage identities with such a myriad of IoT devices. In terms of trust, it is more challenging to rely on IoT devices, which tend to be tampered with easily as they could be mobile devices.

By considering the network layer, IoT ecosystems pose the same wireless networks' general vulnerabilities but are aggravated by the high dynamics, so the requirement for integration becomes difficult with the lack of available standards. With the use of proprietary protocols and the formation of ad hoc network architectures that are not focused to provide security solutions at all layers, accomplishing IoT security goals is very difficult, and this could enable more vulnerabilities that can be exploited by cyber attackers.

The heterogeneity in IoT applications adds more security challenges. Many of the applications need sensitive data like personal information or monitoring data of industrial processes. So the need for protecting the data being trafficked in IoT is very important, so a unique and integrated security framework needs to strive for a customized solution [9]

6.1.3 SECURITY GOALS OF IOT

The security attributes in general—confidentiality, integrity and availability (the CIA triangle)—are required, and specifically with IoT security, these attributes are especially important. Besides that, authentication and access control are other attributes that should be considered as well. By confidentiality of information, only authorized users may read it. By integrity of information, the information must be accurate and unchanged. By availability, the information needs to be available for access by users at any time. By authentication, the user's identity is validated before using a system. By using authorization or access control, an authenticated user gets permission to access a particular resource or information. By imposing all these security attributes, the system will be secure in terms of vulnerabilities and risks, but if any are lacking, security issues can be expected. If the user is not authenticated properly, high vulnerabilities are produced, the attacker can easily get into the system, and different threats can occur. After that, if authentication is done properly but authorization is not, different vulnerabilities and opportunities can be created for the attacker to access any resource in the system and can affect the whole IoT network.

6.1.4 SECURITY REQUIREMENTS IN IOT

By knowing these general security issues affecting the IoT, we can have add security requirements to enhance the security and privacy of the IoT. Accordingly, some security features can be added as well, such as antiviruses, firewalls, security software, etc. Cryptographic algorithms can meet the security requirements, but there is a need for specific algorithms yet to be introduced at the physical layer to meet security requirements [10]. Some of the requirements of security for IoT are as follows:

- Estimation of risks for location, at the time of deploying devices
- Proper use of cryptographic techniques based on vulnerabilities
- Authentication done properly for switching and connected devices to minimize confidentiality issues
- Planning and strategy developed properly for the complete IoT network and not just for a specific area
- Protection of the cloud, as the centralized point for data storage, with proper security (Making data encrypted in the cloud can minimize the risk of stealing the data [11].)
- Use of intelligent techniques of AI and machine learning for reducing human intervention and computational burden [12]
- Centralized environment for communication devices

6.1.5 IOT ENVIRONMENTS

There are vast IoT environments that have been moved from traditional environments to smart environments. Some such environments of IoT have been discussed:

- **Smart Cities:** Smart cities are developed to enhance the quality of life of the people using the emerging communication and computation resources. It involves smart traffic management, smart homes, smart utilities, and smart disaster management and so, on as shown in Figure 6.2. There is a need to transform cities to smart cities in order to have advanced development and smarter management of the whole country. Even though smart cities are intended to enhance the lifestyle of their citizens, there arise many issues to the citizens' privacy. For example, if smart mobility is used, then the location of the user might be traced, or by using smart cards, the user's card details might be at risk [7].
- **Smart Home:** Smart home or home automation is the concept of IoT where different appliances of home and the surroundings are controlled under one point to give users safety, comfort, ease, and security. The quality of life can be improved by adding smartness to the surroundings of home. By implementing automation, information can be collected quickly and passed smoothly among the devices since they are monitored simultaneously. All the devices would be connected at a central point, as illustrated in Figure 6.3. One can monitor all home activities from that central point, and it can be handled from different devices like smartphones, laptops, PCs [13]. By such means, one can access and control activities in the home remotely, an alert message can be sent to the owner in case of danger, and energy consumption of energy at the home can be monitored. Despite of all these



FIGURE 6.2 Smart city components.



FIGURE 6.3 Smart home control under one point.

benefits, we need to look at the security risks such as whether homeowner privacy is compromised or a security threat appears in the IoT network.

- **Smart Industrial Platforms:** With the dramatic increase in the use of IoT applications, people have turned their vision toward automating industrial platforms through IoT. It is the automation of the processes of controlling different departments and tasks in industries such as information collection, remote monitoring, labor. With this platform, the work of industries could be easier, more efficient and reliable. The work hours can be reduced, and the different processes can be connected and monitored through one point. Hence, it has been used in a digital oilfield, a smart grid [4], an intelligent chemical industry, a smart factory, and others. The control system of an industrial IoT enables two-way communication among the control end and remote equipment, centralizing the management and monitoring of decentralized infrastructure [14].
- **Smart Agriculture:** IoT in agriculture is implemented to monitor the soil moisture, select irrigation in dry zones, control micro-climate conditions, and control temperature and humidity. By using such enhanced features of agriculture provided by IoT, farmers can achieve high yields and avoid monetary losses. By having better control of temperature and humidity levels in vegetable and grain production, microbial contaminants and fungus can be prevented, and the quality of crops can be better. However, by involving the cloud for data storage and the IoT environment, the data privacy of the farmer could be at risk [7].

6.2 THREATS ACROSS IOT LAYERS

As illustrated in Figure 6.1, every IoT environment in general involves four layers: (1) A sensing layer deals with the sensor devices for information collection from

surroundings for use by actuators. (2) A network layer is responsible for communication by the establishment of a transmission network. (3) A middleware layer serves as an intermediate layer between the network and application layer and helps in enhancing the storage and computing resources of the two layers. Then gateways are the access points to the layers, and they offer intercommunication among the different services. They are very vulnerable if not properly authenticated. (4) The final layer, the application layer, deals with providing services to end users. The security attacks in these layers are discussed next.

6.2.1 SENSING LAYER ATTACKS

This layer includes a huge number of devices such as actuators, sensors, smart devices. The security attacks and threats are as shown in Figure 6.4 over this layer.

- **Node Capture/Tampering:** This attack could be done by either tempering or replacing a node with a malicious node. The attacker's aim is to get access to and control of the IoT device. An unprotected environment makes it very difficult to capture such attacks. If an attacker get physical access over the node with such attack, any critical cryptographic information can be stolen easily [15].
- **Sleep Deprivation:** IoT nodes have small batteries that make them more vulnerable to DoS attack in which the attacker tries to drain the battery and force the device into a shutdown state, leading to DoS [16]. This can have serious impacts on the functionality of an application such that, in an emergency case, the device would not be able to function and state the emergency. Moreover, the attacker would cause the sleep deprivation attack to the device by running infinite iterative malicious algorithms into the edge devices, keeping the device awake and stopping it from going into sleep mode, ending with sleep deprivation attack [10].
- **Malicious Code Injection Attacks:** This attack is carried out by injecting malicious code into the memory of the device. The attacker can then use such a device as a gateway for performing operations like providing falsified information and hijacking an entire IoT system [10].
- **Side Channel Attacks (SCA):** Most of the time in passive attacks, the goals of attackers are to hack confidential information. Adversaries focus electromagnetic production on the micro-architectures of most of the time processors and other resource consumption to access confidential information. An SCA can be a timing attack or laser-based attack based on power consumption [10]. In current electronics designs, the prevention of an SCA is aimed at the implementation of cryptographic techniques on newer FPGA chips.
- **Eavesdropping:** The authentication mechanism, if not performed as required, may raise an eavesdropping attack possibility, since this information can be passively monitored between the device by an intruder.
- **Bootling Attacks:** When devices are in most of the time bootling process, there is a zero-security level at that time. Specifically for IoT systems,

malicious codes can be easily entered upon booting. Adversaries usually benefit from this state via the sleep-wake cycles during the booting [10].

6.2.2 NETWORK LAYER ATTACKS

the objective of this layer is to reduce communication latency in transmission, but some factors operate on this data in transit. The security attacks in this layer are as follows (Figure 6.4):

- **Phishing Site Attack:** These attacks can be launched over the application deployed over http services. If the ID and password are leaked, this attack can be done easily [10].
- **DoS/DDoS Attacks:** A DoS attack is caused by flooding the target servers with abundant unwanted requests that incapacitate the server from answering. Moreover, it disrupts the server to have communication with the genuine devices, and this results in denial of service. When substrate servers are flooded by using multiple sources, this attack is known as a distributed DoS attack. IoT systems have suitable complexity and heterogeneity, but still the network layer is prone to distributed DoS attacks. Because of the weak configuration of applications and devices, attackers can gain accessible gateways for launching DDoS attacks in the servers [10]
- **Data Transit Attack:** IoT is all about data exchange and the exchange of valuable information that is stored in either the cloud or local servers [10]. This data storage is more vulnerable or highly unsafe if not suitably encrypted. But adversaries find data in transit more irresistible and impuissant. In the IoT system's network layer, data exchange between actuators, sensors, cloud, etc. happen by means of several communication techniques, which makes it more susceptible to data breaches, as illustrated in Figure 6.4.
- **Routing Attack:** A routing attack is the redirecting of communication channels at the time of data transmission. One of the well-known kinds of routing attacks is the sinkhole attack, in which artificial displacement paths tempt devices as their more feasible communication channel. Another kind of routing attack is the wormhole attack, in which a fast transmission path is provided between two devices. An adversary can detour security protocols by the creation of a wormhole between two devices. The wormhole can become a severe attack to an IoT system if combined with any other technique [10].

6.2.3 MIDDLEWARE LAYER ATTACKS

Middleware layer provides the connection between the application and network layers, as shown in Figure 6.4. The security attacks in this layer are as follows:

- **Cloud Flooding Attack:** This attack is similar to a DoS attack in which clouds are flooded with unnecessary requests. Execution of these requests leads to zero quality of service, the depletion of the cloud, and the widespread increase of workload from unfavorable recommendations.

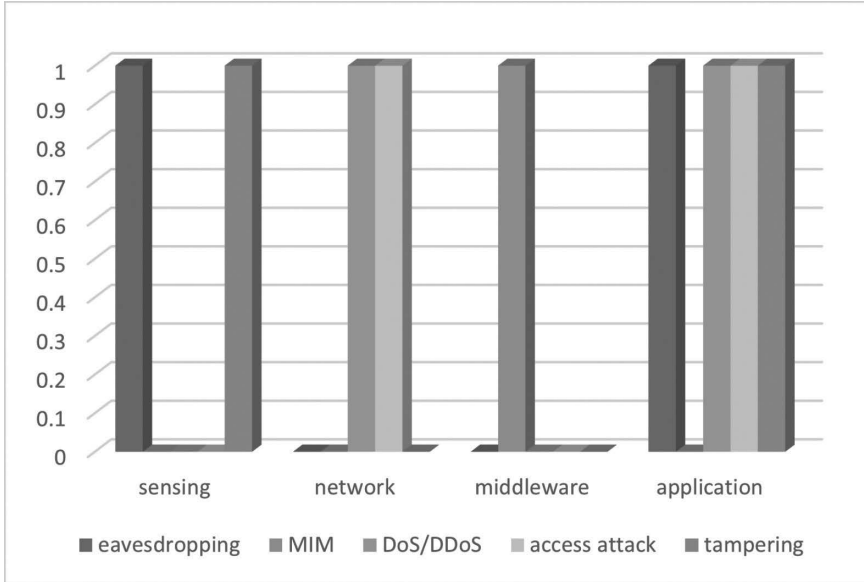


FIGURE 6.4 Common attacks on different layers.

- **Cloud Malware Injection Attack:** The target of this attack is to gain control of the cloud by using malicious code to inject a virtual machine. This virtual machine acts as like a legitimate member of the network in order to obtain access to the services offered by the IoT system.
- **SQL Injection Attack:** In this attack, mischievous commands are embedded in a program in order to get and to modify sensitive information of a user.
- **Man-in-the-Middle Attack:** The attacker acts as an agent between the receiver and sender in an IoT system; as the man-in-the-middle, the attacker could easily gain information from both devices. Similarly, it can access sensitive information and can inject falsified information in the IoT environment. This may lead the attacker to have full control of the system and any client device’s notification.

6.2.4 GATEWAY ISSUES

Gateways are the main entering points for information in the networks. The aim of a gateway is to authenticate devices and applications in order to provide services to end users. Issues at the gateway level are as follows:

- **Extra Interfaces:** Reducing the probability of attacks could only be the possible way in the security of IoT specifically during the new devices’ installation. If some of the functions and services are restricted for users, breaches in backdoor authentication and information can be minimized [10].

- **End-to-End Encryption:** Establishing a reliable and highly secure channel is possible by developing high-profile end-to-end encryption. Because of this, only legitimate users can decrypt the encrypted information. Gateways translate data or information because of inter-switching protocols, and therefore the decryption of enciphered information makes the gateway even more vulnerable to data breaches.
- **Firmware Updates:** In general, many IoT devices are resource constrained in terms of spectrum and power even though they do not have the power of decision making when it comes to installing firmware. The installation of updates depends on gateways by simple validity checking.

6.2.5 APPLICATION LAYER ATTACKS

Services are provided by the application layer to the user. The security attacks in the application layer are as follows (Figure 6.5):

- **Access-Control Attacks:** Access control relates to the authorization of the authenticated users. If this access is compromised, the whole IoT system is susceptible.
- **Reprogramming Attack:** Attackers can reprogram IoT objects in embedded-firmware-based devices and achieve their aims by hijacking the whole system.
- **Sniffing Attacks:** Sniffing into the applications lets the adversaries gain knowledge of the network traffic and sometimes learn passwords and usernames, making the system vulnerable. The adversaries can gain access to confidential information if the system is left with no security [10].

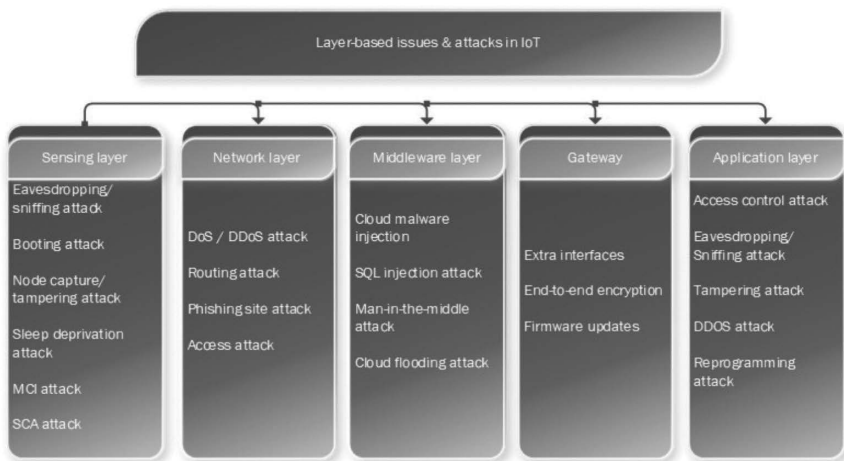


FIGURE 6.5 Layer base security attacks in IoT.

6.3 SOLUTIONS TO IOT SECURITY THREATS

Many different types of solutions have been introduced for addressing different security issues in IoT. By identifying the preceding security issues and attacks, we now discuss the different kinds of solutions to address security issues in IoT: (1) approaches to address security attacks in the different layers of IoT, (2) approaches to meet the security goals of IoT, and (3) current technologies to address security issues in IoT.

6.3.1 APPROACHES TO ADDRESS SECURITY ATTACKS IN IOT LAYERS

Many researchers have worked on producing solutions to minimize the occurrence of security attacks in IoT networks. Different architectures, methods, algorithms, and techniques have been used for addressing the security attacks being faced in the different layers of IoT are shown in Table 6.2.

TABLE 6.2
Solutions to Security Attacks in IoT Layers

No.	Reference	Advantages	Address	Year
1	[17]	Identity leaker for the data owner	Prevents privacy leakage by providing accountability mechanism	2022
2	[18]	Uses cluster-structure-based routing protocol	Security issues like routing attacks	2022
3	[19]	Has low communication and computational costs, prevents unauthorized users from accessing sensors of IoT	Prohibits unreliable authentication; prevents DoS, man-in-the-middle, and modification attacks in healthcare	2022
4	[20]	Efficient computation costs, user anonymity, session key forward secrecy	Prevents node capture attack, impersonation attacks in the smart home	2022
5	[21]	Performs better than algorithms-J48, random forest, random tree in terms of accuracy, precision, FI score, and recall metrics	Prevents LR DoS attacks	2022
6	[22]	Uses decentralized attribute-based access control, which tackles the centralization issue	Tackles privacy issues and access control attacks	2021
7	[23]	Provides reliable access control mechanism and is a more fine-grained mechanism	Prevents access control attacks	2021
8	[24]	Uses multimodal encrypted biometric traits for authentication and homomorphic encryption	Encryption of user data providing reliable authentication	2021
9	[25]	Uses cluster-based IDS	Prevents routing attack such as sinkhole attack and selective forwarding	2019
10	[26]	Uses 3DES algorithm, preventing unauthorized access	Prevents eavesdropping, brute force, DoS in the smart home	2019

TABLE 6.3
Solutions to Meet Security Goals of IoT

No	Ref.	Advantages	Addressing	Year
1	[27]	Gives effective authentication by combination of modular square root algorithm with blockchain	Prevents security and privacy issues	2022
2	[28]	Flexible access control and high throughput	Resists security issues due to vulnerabilities in IoT	2022
3	[23]	Provides reliable access control mechanism and is more fine-grained mechanism	Access control mechanism for industrial IoT, preventing access control attacks	2021
4	[22]	Has decentralized attribute-based access control, which tackles centralization issue	Tackles privacy issues and access control attacks	2021
5	[29]	Ensures user privacy by using identity management mechanism	Prevents authentication issues in IoT	2020

6.3.2 CURRENT APPROACHES TO MEET SECURITY GOALS OF IoT

The security goals of IoT, as mentioned in section 6.1.4, include the CIA triangle along with access control and authentication mechanisms. Various security issues have been identified, some of which are due to improper authentication mechanisms, improper authorization techniques, or other security aspects. Therefore, for overcoming the security issues due to the compromising of such security aspects, certain solutions have been proposed that, when implemented in the IoT, can enhance the security aspects and hence the security goals of the IoT. The solutions are mentioned in Table 6.3.

6.3.3 CURRENT TECHNOLOGIES TO ADDRESS SECURITY THREATS IN IoT

Various technologies are used to secure communications in IoT environments. We discuss machine learning, artificial intelligence, edge computing, and blockchain to provide solutions for securing IoT environments, as discussed in Table 6.4.

- **Blockchain:** Blockchain combined with the IoT has had a great effect on the communication industry. The focus of these two technologies is to improve the overall visibility, transparency, level of trust, and level of comfort for users. IoT devices offer real-time data from sensors, and blockchain offers the key for security of data by the use of a distributed, shared, and decentralized ledger [7].

Blockchain involves the use of public and private keys in communication; hence, only intended nodes can access the data. As the data is encrypted, even if an unintended node is able to access the data, the data contents remain inexplicable [27], leading to the handling of different security issues faced in IoT environments. IoT applications like industrial IoT includes the use of a large number of devices. So, for the cost and traffic issues, blockchain provides effective solutions. The authors in [30] provided

TABLE 6.4
Advanced Technologies to Address Security Issues in IoT

No.	Reference	Address	Technology	Year
1	[34]	Prevents bot attacks in IoT	AI	2022
2	[32]	Security issues	Edge computing	2022
3	[31]	Malware attacks	Machine learning	2021
4	[35]	Security issues	Machine learning	2020
5	[33]	Secured communication	Edge computing	2022
6	[30]	Security issues, access control, and centralization issues	Blockchain	2019
7	[21]	Prevents LR DoS attacks	AI	2022
8	[27]	Prevents privacy and security issues, spoofing attacks	Blockchain	2022
6	[22]	Has decentralized attribute-based access control, which tackles centralization issue	Tackles privacy issues and access control attacks	2021

solution that will move towards decentralization and enable the IoT devices to directly communicate with one another, eliminating the centralization issue [22]. In addition, the blockchain method can prevent the occurrence of many security attacks by providing effective authorization and authentications [28, 29]. Thereby, it can minimize the spoofing attacks such that in such an attack, a malicious node is entered into the IoT network and tries to act like a legitimate one. But, with blockchain use, all legitimate devices are registered on blockchain and can authenticate one another easily without a central broker [27].

- **Machine Learning:** Machine learning is being used in many areas and gaining much interest. Similarly, it is being used for enhancing security in the IoT. Machine learning provides different approaches to protect devices in IoT cyber attacks. Machine learning provides a number of solutions to overcome such attacks as discussed in section 6.2, which are of great concern. One of the techniques is provided in [31], which is the use of dynamic power management architecture. In this approach, dynamic voltage and frequency scaling (DVFS) states were demonstrated, and its feature of variations in runtime provides security to IoT devices against malware attacks, as shown in Table 6.4.
- **Edge Computing:** In edge computing, when used in the IoT, all the data is processed and stored in a local network or within the device. Data is not transferred between the data originator and the processor. Therefore, no data is in transit, hence preventing attacks such as data-in-transit, data breaches, and data theft [7]. Peiying et al. [32] have proposed a solution that uses data disturbance along with the firefly algorithm to enhance security and privacy in the IoT. Another solution was posed in [33] to secure the IoT

communications. This solution is a technique based on a decision tree and is user centric.

- **Artificial Intelligence:** Artificial intelligence or AI technology, when incorporated in IoT, elevates the IoT potential to a high level. It helps the IoT devices and the IoT network in developing decision-making capabilities, predicting the future, and continuously improving performance. This helps in reducing malware attacks in IoT as they can be predicted sooner. For such purposes, a solution using AI has been proposed in [21] that uses feed-forward convolutional neural network for anomaly detection in IoT. This solution is targeted to reduce the occurrence of low-rate DoS attacks in IoT. Similarly, another technique is proposed in [34] that prevents bot attacks in industrial IoT by using a secure network model using VHN technologies.

6.4 SURVEY ANALYSIS

Although the security threats have been identified across the different layers of IoT networks, there are many possible security threats in each layer of the IoT. All the commonly occurring threats to IoT security have been identified and discussed. All these security attacks make the IoT system vulnerable and insecure to use for mission-critical applications [36].

Proposing different kinds of solutions to overcome these attacks, researchers have introduced many. Some have introduced cryptographic techniques to provide enhanced encryption, some have introduced malware detections to detect the threats earlier, and some have introduced advanced architectures that tighten up security in the IoT. But one such solution cannot meet all the security requirements and make an IoT system fully secured. Each of them has tradeoffs [37].

Similarly, we have suggested many solutions to security threats based on advanced technologies like blockchain, machine learning, AI, and edge computing. Although they provide security for IoT systems, they also have some drawbacks—some security issues and performance issues in the use of edge computing, blockchain, machine learning.

The security of blockchain depends on how it is implemented and how the hardware and software are used in that implementation. As the transactions in blockchain made by users are all public, there is the chance that users' private data can be leaked. Also, with the increase of miners, the size of blockchain also increases, which decreases the speed of distribution across the network and increases storage cost. This in turn leads to issues such as availability and scalability in blockchain [38].

There are many algorithms of machine learning, and it is difficult to choose a suitable one for IoT security. If a wrong algorithm is selected, it may give useless output or at least inaccurate and ineffective output. The success of a solution by machine learning depends on such factors, as well as on the diversity of the data selected. Also, the historical data might include missing values, ambiguous values, and meaningless data points. A huge amount of data is being created by the IoT systems; hence it is difficult to preprocess and clean that data with accuracy. Many features, such as removing redundancies, attributing creation, and linear regression, need to be considered in order to use machine learning effectively for IoT security. For edge

computing, user privacy and data security are the main issues. The private data of a user can be leaked and misused if the home in which IoT devices are deployed is subjected to security attacks. Therefore, the user should be aware of measures such as securing Wi-Fi connections. Also, the user should own fully the data at the edge or have control of data sharing [39].

6.5 FUTURE RESEARCH DIRECTIONS

These are some of the research directions for future.

The gateways among the layers of an IoT system must be secured, or they provide easy entry points that attackers can use to attack the IoT system. End-to-end encryption might be a more promising solution for securing the data passing via gateways than the use of specific encryption techniques.

Edge devices in the IoT are the most resource-constrained devices and are hence vulnerable to attacks. The studies show that, while little power is needed to implement suitable security practices for edge nodes, they are still very vulnerable to many attacks.

More reliable and efficient consensus methods could be designed for reaching consensus on the devices, along with avoiding the extensive use of computation power. The existing algorithms are extremely resource-hungry and are less efficient.

6.6 CONCLUSION

IoT is becoming much more popular, and its number of devices is increasing dramatically. With the increase of devices, the complexity of IoT systems is increasing as well. Since IoT devices are becoming more complex, cheaper, highly distributed, and heterogeneous, more security issues are on the rise. In this chapter, various security issues and attacks have been identified at the various layers of an IoT network. The issues have been covered related to the application layer, gateways, middleware layer, network layer, and sensing layer. Also, the existing solutions to security threats of IoT have been discussed, which include blockchain, edge computing, machine learning, and AI. Many open issues and future research directions for the security enhancement of the IoT have also been discussed. This chapter is expected to serve as an important resource for enhancing security in upcoming IoT systems.

REFERENCES

- [1] M. Arif Khan, Sabih Ur Rehman, Muhammad Ashad Kabir, Muhammad Imran, Samrah Arif, "Investigating Smart Home Security: Is Blockchain the Answer?," *IEEE Access*, vol. 8, no. 1, pp. 117802–117816, 2022.
- [2] Mahmoud Abdelsalam, Sajad Khorsandroo, Sudip Mittal, Maanak Gupta, "Security and Privacy in Smart Farming: Challenges and Opportunities," *IEEE Access*, vol. 8, no. 1, pp. 34564–34584, 2020.
- [3] Pierfrancesco Bellini, Angelo Difino, Paolo Nesi, Claudio Badii, "Smart City IoT Platform Respecting GDPR Privacy," *IEEE Access*, vol. 8, no. 1, pp. 23601–23623, 2020.

- [4] Abouzar Estebarsari, Enrico Pons, Marco Pau, Stefano Quer, Massimo Poncino, Lorenzo Bottaccioli, Edoardo Patti, Matteo Orlando, "A Smart Meter Infrastructure for Smart Grid IoT Applications," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12529–12541, 2022.
- [5] Sahil Garg, Georges Kaddoum, Bong Jun Choi, Geetanjali Rathee, "Decision-Making Model for Securing IoT Devices in Smart Industries," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4270–4278, 2021.
- [6] J. Morrish and M. Arnott, "Global IoT Forecast Report, 2021–2030," Transforma Insights, 2022 [Online]. Available: <https://transformainsights.com/research/reports/global-iot-forecast-report-2032>.
- [7] Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, Biplab Sikdar, Vikas Hassija, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, no. 1, pp. 82721–82743, 2019.
- [8] Shabana Mehfuz, Shabana Urooj, Sonam Lata, "Secure and Reliable WSN for Internet of Things: Challenges and Enabling Technologies," *IEEE Access*, vol. 9, no. 1, pp. 161103–161128, 2022.
- [9] Egberto A. R. de Oliveira, Fabio H. Silva, Rui R. Mello, Felipe M. G. França, Flavia C. Delicato, José F. de Rezende, Luís F. M. de Moraes, Evandro L. C. Macedo, "On the Security Aspects of Internet of Things: A Systematic Literature Review," *Journal of Communications and Networks*, vol. 21, no. 5, pp. 444–457, 2019.
- [10] Azlan Awang, Samsul Ariffin BIN Abdul Karim, Naqash Azeem Khan, "Security in Internet of Things: A Review," *IEEE Access*, vol. 10, no. 1, pp. 104649–104670, 2022.
- [11] Peng Xu, Laurence Tianruo Yang, Wei Wang, "Secure Data Collection, Storage and Access in Cloud-Assisted IoT," *IEEE Cloud Computing*, vol. 5, no. 4, pp. 77–88, 2018.
- [12] Kai Xu, Naiyu Wang, Jianlin Jiao, Ning Dong, Meng Han, Hao Xu, Xianfei Zhou, "A Secure and Privacy-Preserving Machine Learning Model Sharing Scheme for Edge-Enabled IoT," *IEEE Access*, vol. 9, pp. 17256–17265, 2021.
- [13] Vinod Kumar Shukla, Ruchika Bathla, Sameera Ibrahim, "Security Enhancement in Smart Home Management Through Multimodal Biometric and Passcode," in *2020 International Conference on Intelligent Engineering and Management (ICIEM)*, 2020, IEEE, London, United Kingdom, pp. 420–424.
- [14] Hanyi Zhang, Minghui Li, Chunpeng Ge, Liang Liu, Zhe Liu, Liming Fang, "A Secure and Fine-Grained Scheme for Data Security in Industrial IoT Platforms for Smart City," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 7982–7990, 2020.
- [15] Suhaib Obeidat, Jennifer Holst, Abdullah Al Hayajneh, Joseph Brown, Muath A. Obaidat, "A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures," *Computers*, vol. 9, no. 44, pp. 1–43, 2020.
- [16] M. Frustaci, P. Pace, G. Aloï, G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," *IEEE Internet Things*, vol. 5, pp. 2483–2495, 2018.
- [17] Xianxian Li, Peng Liu, Wangjie Qiu, Chuanjian Yao, Bo Yuan, Chunpei Li, "Efficient and Traceable Data Sharing for the Internet of Things in Smart Cities," *Computers and Electrical Engineering*, vol. 103, 2022.
- [18] Fang B. Xian Wen, Celestine Iwendi, Li-li F. Wang, Syed Muhammad Mohsin, Zhaoyang Han, Shahab S. Band, Sohaib A. Latif, "AI-Empowered, Blockchain and SDN Integrated Security Architecture for IoT Network of Cyber Physical Systems," *Computer Communications*, vol. 181, no. 1, pp. 274–283, 2022.
- [19] Gurjot Singh Gaba, Karanjeet Choudhary, M. Shamim Hossain, Mohammed F. Alhamid, Ghulam Muhammad, Mehedi Masud, "Lightweight and Anonymity-Preserving User

- Authentication Scheme for IoT-Based Healthcare,” *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2649–2656, 2022.
- [20] Qiang Cao, Chenyu Wang, Zifu Huang, Guoai Xu, Shihong Zou, “A Robust Two-Factor User Authentication Scheme-Based ECC for Smart Home in IoT,” *IEEE Systems Journal*, vol. 16, no. 3, pp. 4938–4949, 2022.
- [21] Maode Ma, Rong Su, Harun Surej Ilango, “A FeedForward—Convolutional Neural Network to Detect Low-Rate DoS in IoT,” *Engineering Applications of Artificial Intelligence*, vol. 114, pp. 1–9, 2022.
- [22] Volkan Dedeoglu, Salil S. Kanhere, Raja Jurdak, Aleksandar Ignjatovic, Guntur Dharma Putra, “Trust-Based Blockchain Authorization for IoT,” *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, p. 1646, 2021.
- [23] Thanh Kim Pham, Maanak Gupta, James Benson, Jaehong Park, Ravi Sandhu, Smriti Bhatt, “Attribute-Based Access Control for AWS Internet of Things and Secure Industries of the Future,” *IEEE Access*, vol. 9, pp. 107200–107223, 2021.
- [24] Mahmoud Elkhodr, Fariza Sabrina, Farhad Ahamed, Ergun Gide, Farnaz Farid, “A Smart Biometric Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services,” *Sensors*, vol. 21, no. 552, pp. 1–18, 2021.
- [25] Nishtha Kesswani, Sarika Choudhary, “Cluster-Based Intrusion Detection Method for Internet of Things,” in *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 2019, IEEE, Abu Dhabi, UAE, pp. 1–8.
- [26] F. James, “IoT Cybersecurity based Smart Home Intrusion Prevention System,” in *2019 3rd Cyber Security in Networking Conference (CSNet)*, 2019, IEEE, Quito, Ecuador, pp. 107–113.
- [27] Xuechao Yang, Xun Yi, Ibrahim Khalil, Xiaotong Zhou, Debiao He, Xinyi Huang, Surya Nepal, Xu Yang, “Blockchain-Based Secure and Lightweight Authentication for Internet of Things,” *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3321–3332, 2022.
- [28] Ning Xu, Haibin Zhang, Wen Sun, Abderrahim Benslimane, Peng Wang, “Dynamic Access Control and Trust Management for Blockchain-Empowered IoT,” *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 12997–13009, 2022.
- [29] Huisen Liu, Liehuang Zhu, Ke Xu, Hongbo Yu, Xiaojiang Du, Mohsen Guizani, Meng Shen, “Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.
- [30] Kashif Sharif, Fan Li, Sabita Maharjan, Saraju P. Mohanty, Yu Wang, Sujit Biswas, “PoBT: A Lightweight Consensus Algorithm for Scalable IoT Business Blockchain,” *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 1–13, 2019.
- [31] Arvind Singh, Harshit Kumar, Monodeep Kar, Saibal Mukhopadhyay, Nikhil Chawla, “Securing IoT Devices Using Dynamic Power Management: Machine Learning Approach,” *IEEE Internet of Things Journal*, vol. 8, no. 22, pp. 16379–16394, 2021.
- [32] Yaqi Wang, Neeraj Kumar, Chunxiao Jiang, Guowei Shi, Peiying Zhang, “A Security-and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems,” *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 97–108, 2022.
- [33] Stanly Wilson, Ashish Nanda, Ming Liu, Srinibas Swain, Biswa P. S. Sahoo, Kumar Yelamarthi, Prashant Pillai, Hesham El-Sayed, Mukesh Prasad, Deepak Puthal, “Decision Tree Based User-Centric Security Solution for Critical IoT Infrastructure,” *Computers and Electrical Engineering*, vol. 99, 2022.
- [34] Konstantinos E. Psannis, Zhihan Lv, Vasileios A. Memos, “A Secure Network Model Against Bot Attacks in Edge-Enabled Industrial Internet of Things,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 7998–8006, 2022.

- [35] B. J. D. Mohanta, “Internet of Things Security Using Machine Learning,” in *Advances in Machine Learning and Computational Intelligence, Proceedings of ICMLCI 2019*, 2021, Springer, Singapore, pp. 129–136.
- [36] Ochanya S. Ogbah, Shivanand Guness, Xavier Bellekens, Amar Seeam, “Threat Modeling and Security Issues for the internet of things”.
- [37] Sitara Anumotu, Pronika, Kritika Soni, Kushagra Jha, “Security Issues and Architecture of IOT,” in *Proceedings of the International Conference on Artificial Intelligence and Smart Systems (ICAIS-2021)*, 2021, IEEE, Coimbatore, India, pp. 1381–1385.
- [38] Mahmoud Abdelsalam, Sajad Khorsandroo, Sudip Mittal, Maanak Gupta, “Security and Privacy in Smart Farming: Challenges and Opportunities,” *IEEE Access*, vol. 8, pp. 34564–34584, 2020.
- [39] Hemraj Saini, Punit Gupta, Anouar Ben Mabrouk, Dinesh Kumar Saini, “Prediction of Malicious Objects Using Prey-Predator Model in Internet of Things (IoT) for Smart Cities,” *Computers & Industrial Engineering*, vol. 168, 2022.

7 Intrusion Detection System Using AI and Machine Learning Algorithm

Muhammad Tehmasib Ali Tashfeen

7.1 INTRODUCTION

There are numerous different kinds of threats on the web, such as malware and distributed denial of service assaults. An intrusion detection (IDS) system can defend a network against such threats. An IDS system is capable of detecting intrusions, and when it does, it issues an alarm. This intrusion detection system for networks examines all traffic. This might be a challenging undertaking for big data centers [1]. The infrastructure of a data center contains a large amount of information. Conventional intrusion detection systems cannot filter out every bit of communication.

Using IP streams to regenerate data packets is one technique to resolve such issues. A technology for intrusion detection can monitor every communication if IP channels are used. A huge amount of upkeep is needed for intrusion detection systems. In addition to being expensive, this is course dependent. Furthermore, the digital storage of critical data is growing. These brand-new services may all have security issues that allow credentials or other confidential material to be exposed, as well as other private information [2]. Due to the potential for such severe consequences, security weaknesses become increasingly significant. Confidential information leakage is not the only problem; virus protection for a system or network is, however, crucial.

Given that, it is especially crucial to be able to recognize and stop assaults on enterprise networks. For this, intrusion detection systems are employed. Administrators can be notified of harmful activity via an intrusion detection system. Most intrusion detection systems necessitate a significant amount of human upkeep to function well [3]. This study examines whether an intrusion detection system can function well straight out of the package. Methods for machine learning are used to accomplish this. These programs can recognize correlations in data. Methods using machine learning appear to have promise for such issues of autonomous intrusion detection. This study attempts to show how an intrusion detection system might function well right out of the box [4–5]. Machine learning methods are employed to achieve this. These are programs that can pick up on correlations and information over time. This

appears to be very relevant to intrusion detection; it will also be shown in this study that the techniques might or might not be effective.

7.2 ATTACK CLASSIFICATIONS

To begin with, separating malevolent activity into internal and outward manifestations is a helpful categorization. Human comprehension is facilitated by this. Different categories can be used with the IDS directly. Nonetheless, an administrator must be informed of any detections made by the IDS. It is simpler to comprehend a dichotomy between criminal attacks on the inside and outside [6]. Individual characteristics help to distinguish each kind of malicious conduct. The ability to modify the IDS to improve identification requires knowledge of these traits.

- **External Abnormal Behavior:** Externally aberrant behavior comprises many network assaults of various types. There are several kinds of assaults. Physical assaults, memory overflows, distributed denial of service (DDoS), brute-force cyber attacks, vulnerability assessment, and man-in-the-middle (MITM) attacks are a few of the threats that might be encountered [7].
- **Internal Abnormal Behavior:** Malware is any improper system activity. Malware comes in many different varieties and may be divided into four different groups: Trojan horses, worms, botnets, and viruses [8]. Actual programs referred to as malware infiltrate a computer to carry out a certain function. Which classification a malware falls into is determined by its purpose.
- **Detection:** Just the networks are monitored by NIDS [9], NIDS cannot identify every assault. The first and only assaults that could be identified are those that employ the network. Additionally, flow-based IDSs are limited to employing only data recorded [10–12]. This significantly reduces the number of assaults that may be found. Distributed denial of service, vulnerability assessments, worms, and botnet assaults can all often be found utilizing flow-based intrusion detection network methods [13].

7.3 INTRUSION DETECTION SYSTEM

A device that attempts to ascertain whether a computer is being attacked, in order to identify invasions within a system, is known as an intrusion detection system (IDS). An IDSs are frequently used. Cyber attacks and anomalies are other names for intrusions. An IDS keeps an eye on the system and network activity. IDS can be categorized in one important foundation on how they recognize intrusion.

An intrusion detection system (IDS) is a crucial component of any information security program, helping organizations detect and respond to potential security breaches. In recent years, IDS has evolved into a more comprehensive security tool, integrated with security information and event management (SIEM) solutions [14–15], as shown in Figure 7.1. SIEM is a security solution that provides real-time analysis of security alerts generated from network devices and applications [16, 17].

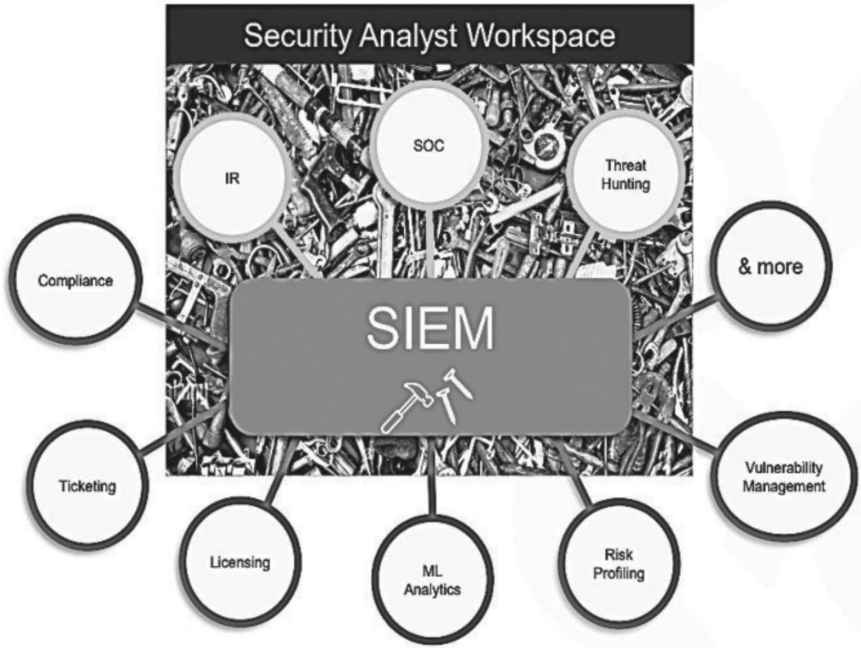


FIGURE 7.1 Growth of SIEM beyond its initial scope.

Integrating IDS with SIEM provides organizations with a more robust security solution. IDS works by monitoring network traffic and analyzing logs and other system data to detect potential threats. SIEM, on the other hand, collects and analyzes security alerts generated by various security tools and devices [18]. By combining the two technologies, organizations can benefit from a more efficient and comprehensive security solution.

IDS can be integrated with SIEM in two primary ways. The first is through a stand-alone IDS solution that can be integrated with SIEM through APIs [19]. The second way is through SIEM solutions that offer built-in IDS capabilities. The latter is becoming increasingly popular as SIEM vendors recognize the importance of IDS integration.

The integration of IDS and SIEM brings several benefits to organizations. First, it enables organizations to centralize their security monitoring and management, making it easier to identify and respond to potential security breaches [20–23]. Second, it provides organizations with a more comprehensive view of their security posture by enabling them to correlate security alerts generated by different security tools and devices [24–25]. Third, it enhances the accuracy of security monitoring by reducing false positives and false negatives, thereby improving incident response times.

Several challenges are associated with integrating IDS and SIEM. First, it requires a significant investment in terms of resources and infrastructure, including hardware, software, and personnel [26]. Second, it requires organizations to develop and implement robust security policies and procedures to ensure the effectiveness of

the integrated solution [27, 28]. Third, it requires organizations to train their security personnel on how to use the integrated solution effectively.

To overcome these challenges, organizations must carefully evaluate their security needs and develop a comprehensive security strategy that takes into account their unique security requirements. This includes conducting a thorough risk assessment, identifying potential threats, and developing appropriate security controls and measures.

In conclusion, IDS and SIEM are two critical components of any effective information security program. By integrating IDS with SIEM, organizations can benefit from a more efficient and comprehensive security solution. While several challenges are associated with IDS-SIEM integration, organizations can overcome them by carefully evaluating their security needs and developing a comprehensive security strategy that takes into account their unique security requirements [29]. Overall, the integration of IDS and SIEM is an essential step toward enhancing an organization's security posture and improving incident response times.

- **Host-Based Intrusion Detection System:** Technologies that examine the machine they are placed in or are physically attached to are called host-based intrusion detection solutions [30]. Administrators can keep track of the system's status using audit trails or by keeping an eye on program execution, among other things. Intrusion detection systems can be constrained by audit trails because of how extensively they depend on them [31]. The total quantity of audit logs may also be a problem [32]. Every observed log has to be processed, which implies that if HIDS is placed inside, it might significantly affect the client operation of the system.

A further drawback is that every weakness that results in an alteration in the audit reports also affects the HIDS's trustworthiness. The HIDS is unable to view and identify what occurred if an auditing record is altered.

- **Network-Based Intrusion Detection System:** Internet intrusion detection systems are installed at specific locations inside an infrastructure to watch over traffic to and from interfaces. These function by employing the same theory as wiretapping. Hackers "tap" into a connection and monitor every bit of conversation [33]. Although the threat is lessened, the intrusive party might attempt to reduce his system functions. NIDS are independent of the OS they use to track network activity [34]. To assess whether the information is malignant, the computer can analyze traffic using several methods. The network data may be analyzed in two distinct methods. Every full packet, such as flags and contents, is used in packet-based assessment [35–37]. Packet-based intrusion detection and prevention is a type of system for intrusion detection that uses packet-based analyses. The fact that a variety of information is available for this kind of study is advantageous. To detect whether such a transmission is malevolent and should be either accepted or rejected, every individual byte in the payload might be examined. Instead of using system EM, the flow-based statement makes use of generalized data collected about real networks. A flow-based network intrusion detection system uses flow-based analysis to identify intrusions [38]. This flow

is determined as a solitary link between both the hosts and maybe another piece of equipment.

- **Intrusion Prevention System:** An intrusion detection system with the capacity to stop intrusions is known as an intrusion prevention system (IPS/IDPS) [39]. Although it is preferable, an IDS doesn't necessarily have to be capable of recognizing intrusions as they are taking place. Because an IPS must be capable of preventing accidents from occurring, it must also be capable of detecting them in legitimately preventative measures given that the network cyber attack might include cutting off the link, restricting an IP address, or restricting the transmission rate.

Some techniques used to identify such cyber attacks may well be significantly impacted by the requirement that assaults be recognized instantaneously. For instance, an IDS may provide an alarm even if it is unsure that the occurrence for which it is issuing the warning is indeed an abnormality. Before acting, an IPS must be confident about the situation. If not, the IPS could take steps that the company using the IPS doesn't desire [40].

- **Detection:** There are several ways to identify breaches. Some of the techniques are anomaly based and signature based.

Algorithms that rely on signatures verify asserted signatures against a collection of known signatures [41, 42]. Transformed elements from a packet or stream data are put together just to form a signature. An inbound stream or packet is marked as malevolent if its signature matched one in the database. Since signature-based approaches simply attempt to correlate entering signatures to attack patterns in the database, they have little cost in terms of calculation and preprocessing. Since all it does is analyze signatures, network deployment is simple. The system is not required to become familiar with how network traffic appears. Techniques that rely on signatures are highly successful against well-known cyber attacks [43]. Without updating the databases with current signatures, it is impossible to identify emerging risks.

Taking appropriate anomaly-based approaches, also known as behavior-based techniques, can predict the behavior of network activity. A warning is given and the incoming packet is tagged as malevolent when it differs from such a model. Since these approaches employ a statistical method of typical behavior, they ought to be able to spot any anomalies in this pattern. As a consequence, new cyber attacks that go too far from customary behavior are also discovered.

It is impossible to install the system onto an infrastructure and expect it to function because a simulation of the network activity must be constructed [44]. The system must become familiar with the behavior of the network activity, as shown in Figure 7.2. When training data contains errors, including such misclassifications, issues might occur, including the generation of several false positive notifications.

As like an anomaly-based approach, machine learning techniques can be applied. Methods utilizing machine learning do have the ability to extract information from data and determine whether fresh data is malignant [45].

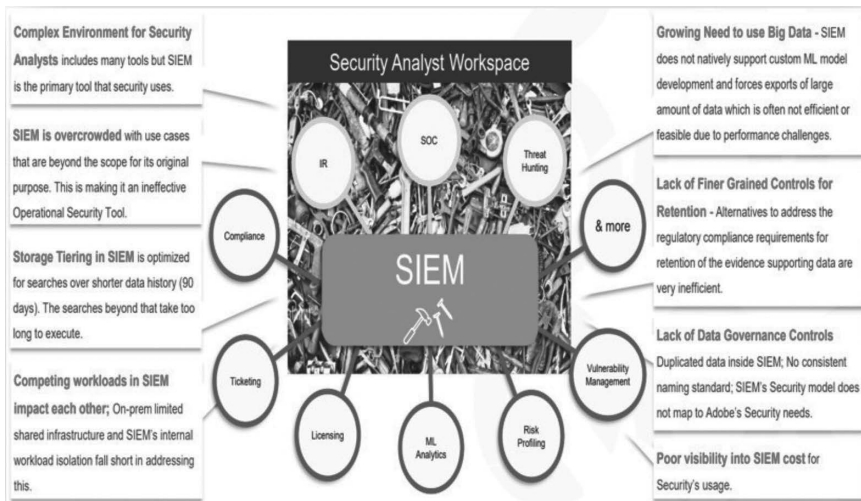


FIGURE 7.2 Security needs a big data platform separate from traditional SIEM to correlate security events in IDS.

7.4 MACHINE LEARNING

Computer science is the discipline of machine learning. This is a part of artificial intelligence that enables computer systems to discover patterns within information. Programs that really can draw from information and make forecasts about it are investigated by machine learning [46]. Such methods are termed machine learning procedures. To use data to create projections, a machine learning system must first train. The program must be taught by being exposed to numerous data samples and the appropriate projections for each case.

The method must be deployed anywhere from a few thousand to around a hundred thousand instances. Once algorithms for machine learning have gained information from the data, it may be applied to certain other information to make forecasts. For instance, machine learning could be applied to monitor a hospital patient's pulse rate [47]. The patient's heartbeat and the timestamp are displayed in the machine-learning model during the training phase. That machine learning system can forecast the patient's expected heartbeat depending on the present time once learning is complete. Contrasting the anticipated heartbeat with the actual pulse rate, this Medical Interoperability Gateway (MIG) is used to evaluate whether the patient's heartbeat is healthy.

- **Evaluating ML for an IDS:** The *F*-score can be combined with the machine learning system to gauge accomplishment [48]. This, though, is insufficient for systems for intrusion detection all on their own. The *F*-scores for accuracy and recall are equally important. While analyzing intrusion detection systems, this isn't always the situation. When a study population is labeled as

an intrusion even if it is truly normal, this is known as just a false positive. Whenever a study population is truly an intrusion and yet is categorized as normal, this is known as a false negative [49, 50]. False negatives are undesirable since they indicate that an intrusion went undetected. But the majority of intrusion detection systems are employed in a tiered manner. This implies that yet another layer may identify an intrusion if the first layer misses it.

The tiered strategy can provide quite different results. Its primary layer attempts to identify as many anomalies as it can (while having a poor recall) before forwarding the information about which incidents have been found to further levels. This strategy indicates that a poor recall is acceptable. Depending on how the IDS will be utilized, a machine-learning-based scoring system is employed.

- **Using ML for IDS:** Whether or not information can be utilized in such a machine-learning system, it must first be evaluated. This implies that characteristics must be picked. Some characteristics can be discovered quickly, while others must be discovered via testing and experimentation. Utilizing every element of a dataset doesn't ensure the IDS will perform at its maximum, as depicted in Figure 7.3 system's processing cost and false alarm rate could both go up as a result [51]. This is because some traits are redundant or aren't necessary to distinguish among various classes.



FIGURE 7.3 Big data at the core of anomaly detection.

7.5 IMPLEMENTATION

- **Technology Stack:** Scikit-learn, a powerful machine learning toolkit for Python, is a frequently used major package. It is based on Matplotlib, SciPy, and NumPy [52]. Again, with a BSD license, it is additionally open source and used for commercial purposes. This toolkit was picked because it provides instructions for the most crucial procedures. Additionally, Scikit-learn includes many tools for visualizing machine learning algorithms, including a graph that displays the learning curve. These could be effective techniques for assessing how well machine learning algorithms function. It also offers techniques to determine the F -score. This is advantageous since it reduces the likelihood that F -score calculation errors will occur [53].
- **Program Execution:** There are several stages in system implementation. The program's components are defined in a Jupyter Notebook. This includes the information that will be utilized in training, verification, machine learning algorithms, etc.

The software may begin the training phase after it has acquired the configuration file. The defined algorithm is utilized and trained to use the provided data in this step. The forecasting phase then begins. This stage makes use of the prediction data and compiles all the findings [54]. Those various phases are reflected in the project's and the components' structures.

- **Structure:** Modularity is included in the system. The machine learning method is the initial one. All machine learning techniques are included in this section. There is an attribute module as well. The methods that can be utilized to extract features from streams are contained in this section, as shown in Figure 7.4. All the modules needed to import the information from the various datasets are contained in a loading module [55].

The many classes in use for training are included in a training module. Those classes provide the information for the algorithm for machine learning via a loaders class. They specify which information should be utilized, such as excluding normal behavior and utilizing only deviant behavior.

There's a findings section at the end. This section must log or visually represent all of the results from machine-learning algorithms.

- **Datasets:** UNSW-NB 15 datasets are used to evaluate the techniques and their implementations. Various aspects of such machine learning algorithms are tested with this database. To start learning, a portion of a dataset must be selected and fed into the machine learning methods. The algorithm is then evaluated using the procedure and a different sample of the exact dataset.

The methods are evaluated utilizing datasets from the actual world. The methods were finally evaluated utilizing unlabeled, unprocessed actual information in the fourth stage. This guarantees that perhaps the algorithm works effectively with raw, actual statistics. The machine learning methods have indeed been put to the test using various datasets.

The UNSW-NB15 dataset is a network traffic dataset that is widely used for intrusion detection system (IDS) evaluation. Created by the Cyber Range Lab at the University of New South Wales (UNSW), Australia, this dataset includes normal traffic and various types of attacks such as

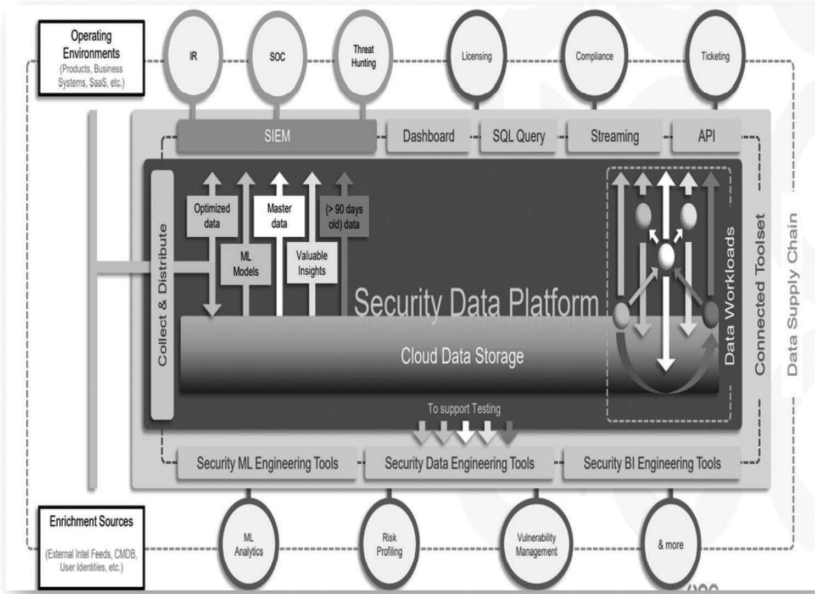


FIGURE 7.4 Security data platform’s holistic view.

denial-of-service (DoS), port scanning, and data exfiltration. The dataset contains a total of 2.5 million network flows, captured over nine hours, using a custom-built network sensor, as shown in Figure 7.5. The dataset is available in both raw and preprocessed formats and includes features such as packet headers, flow statistics, and payload data. Due to its realistic and diverse nature, the UNSW-NB15 dataset is frequently used as a benchmark dataset in academic research and industry evaluations of IDS and machine-learning-based intrusion detection systems (ML-IDS).

- **Algorithm Selection:** An intrusion detection system (IDS) is a security solution that monitors and analyzes network traffic and system activity to identify potential security threats or malicious activities [56]. IDSs can be either signature based, where they compare observed events with pre-defined patterns, or behavior based, where they compare observed events with established normal behaviors. The selection of the algorithm used in an IDS depends on various factors such as the nature of the network, the type of threats, and the computational resources available [57].

One of the most widely used algorithms for IDS is the rule-based system, which is a signature-based approach. In this approach, the IDS searches for predefined patterns or rules in network traffic to identify known attacks [58]. This method is often used in combination with machine learning algorithms, which allow for the automated learning of patterns and behaviors. However, the rule-based system can be less effective against new or unknown attacks, which may not match the predefined rules.

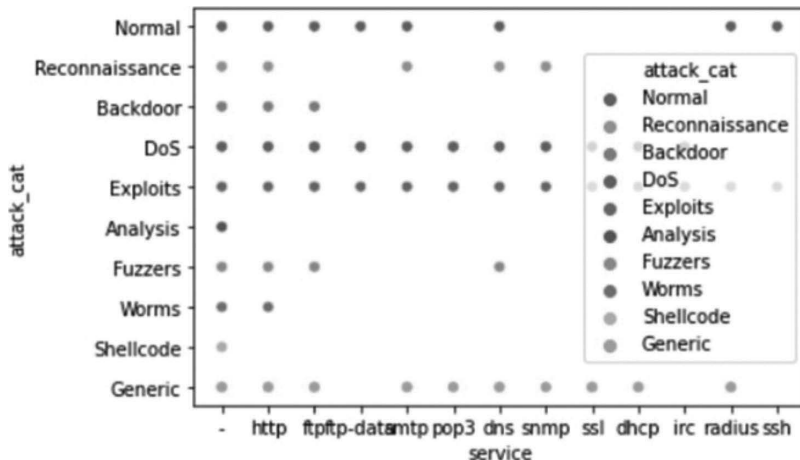


FIGURE 7.5 Dataset classified by attack category.

Another approach to IDS is anomaly-based detection, which compares the observed behavior of network traffic against an established normal behavior. This approach can be more effective at identifying unknown attacks or deviations from normal behavior, but it can also result in more false positives [59]. To address this issue, anomaly-based detection algorithms often employ statistical or machine learning techniques to refine the detection of anomalies.

Machine learning algorithms have gained popularity in IDS due to their ability to automatically learn and adapt to new threats. These algorithms can be either supervised, where they are trained on labeled datasets, or unsupervised, where they are trained on unlabeled datasets [60]. Supervised machine learning algorithms, such as decision trees, support vector machines (SVMs), and neural networks, can be used to classify network traffic as normal or malicious based on previously labeled data [61]. Unsupervised machine learning algorithms, such as clustering and association rule mining, can be used to detect abnormal behavior or new attacks that do not match preexisting patterns.

Deep learning algorithms, a subset of machine learning, have also been used in IDS to analyze large datasets and detect complex attacks. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two popular deep learning techniques used in IDS [62]. CNNs are particularly effective at analyzing packet headers, while RNNs can be used to analyze temporal data, such as system logs.

In summary, the selection of an algorithm for IDS depends on various factors, such as the type of network, the nature of the threats, and available computational resources. A combination of different techniques, such as rule-based and machine-learning-based approaches, may be necessary to provide comprehensive coverage against a wide range of threats. Ultimately,

the choice of algorithm will depend on the specific needs and objectives of the organization deploying the IDS.

- **Unsupervised Learning:** Unsupervised learning is a type of machine learning that involves analyzing data without any prior knowledge of the expected outcomes or labels. In an intrusion detection system (IDS), unsupervised learning algorithms can be used to detect unknown or novel attacks that may not match preexisting patterns or signatures [63–65]. In this approach, the IDS identifies anomalies or deviations from normal behavior in the network traffic, which may indicate potential security threats or malicious activity.

One common unsupervised learning technique used in IDS is clustering, which involves grouping similar data points based on their characteristics. Clustering can be used to identify groups of network traffic that are similar in behavior or to detect new types of traffic that do not match existing patterns [66]. One example of a clustering algorithm used in IDS is *K*-means clustering, which partitions the data into *K* clusters based on the distance between data points.

Another unsupervised learning technique used in IDS is association rule mining, which involves discovering interesting relationships or patterns in the data. Association rule mining can be used to identify sequences of events or activities that are associated with malicious behavior [67]. For example, if an attacker is attempting to exfiltrate data from a system, association rule mining may detect a pattern of high outbound traffic to an unfamiliar destination.

Principal component analysis (PCA) is another unsupervised learning technique that can be used in IDS. PCA involves reducing the dimensionality of the data by identifying the most important features or variables that explain the majority of the variance in the data [68]. This can be useful for identifying patterns or anomalies in the data that may not be immediately apparent in the original data. For example, PCA can be used to identify unusual patterns in network traffic, such as unusual data transfer rates or packet sizes.

One challenge of unsupervised learning in IDS is the issue of false positives, which can occur when the algorithm identifies normal behavior as anomalous or malicious [69]. This can be especially problematic in unsupervised learning, where there is no prior knowledge of the expected outcomes or labels. To address this issue, unsupervised learning algorithms often require a human expert to review and validate the results.

Another challenge of unsupervised learning in IDS is the computational complexity of the algorithms, which can be resource intensive and may require specialized hardware or software [70]. This can make unsupervised learning approaches less practical for real-time or high-performance IDS.

In conclusion, unsupervised learning algorithms can be a valuable tool in an intrusion detection system for detecting unknown or novel attacks. Clustering, association rule mining, and PCA are common unsupervised learning techniques used in IDS [71]. However, the issue of false positives and computational complexity should be considered when selecting and

deploying unsupervised learning algorithms in an IDS. A combination of supervised and unsupervised learning approaches may be necessary to provide comprehensive coverage against a wide range of threats.

- **Supervised Learning:** Supervised learning is a popular approach used in intrusion detection systems (IDS) to classify network traffic as normal or malicious based on previously labeled data. This approach involves training a machine learning model on a dataset of labeled examples, where each example is labeled as either normal or malicious. Once the model is trained, it can be used to classify new instances of network traffic as either normal or malicious.

One commonly used supervised learning algorithm in IDS is the decision tree. A decision tree is a model that predicts the class of an instance by recursively splitting the data into smaller subsets based on the values of different features [72]. The tree is constructed based on the most informative features that have the greatest impact on the classification task. Once the tree is constructed, it can be used to classify new instances of network traffic based on their feature values.

Another popular supervised learning algorithm used in IDS is the support vector machine (SVM) [73]. SVMs are a type of binary classifier that separates data into two classes based on a hyperplane that maximizes the margin between the classes. The SVM algorithm attempts to find the optimal hyperplane that separates the classes and minimizes classification errors. SVMs are particularly effective in high-dimensional spaces and can handle both linear and nonlinear data.

Artificial neural networks (ANNs) are also commonly used in supervised learning for IDS. ANNs are a set of interconnected nodes that can be used to model complex functions [74]. These networks consist of input, hidden, and output layers, where each node in the input layer represents a feature of the data, each node in the hidden layer performs a mathematical operation on the input data, and each node in the output layer represents the final classification decision. ANNs can be trained using a backpropagation algorithm, which adjusts the weights between nodes to minimize classification errors.

One important consideration when using supervised learning in IDS is the availability and quality of labeled data. Labeled data is often scarce and may not represent the full range of malicious activity that an IDS may encounter [75]. Furthermore, malicious attackers may change their tactics and strategies over time, making it difficult to keep labeled datasets up-to-date. To address these challenges, researchers have developed various techniques for generating synthetic data and adapting models to evolving threats.

Another challenge of supervised learning in IDS is the risk of overfitting. Overfitting occurs when a model is trained on a limited set of data and becomes too specialized to that data, resulting in poor performance on new data. Regularization techniques, such as L1 and L2 regularization, can be used to prevent overfitting by adding a penalty term to the loss function that encourages simpler models [76].

In summary, supervised learning is a powerful approach to intrusion detection that can be used to classify network traffic as normal or malicious based on labeled examples. Decision trees, SVMs, and ANNs are popular algorithms used in supervised learning for IDS. However, the availability and quality of labeled data and the risk of overfitting are important considerations when using this approach.

7.6 LITERATURE REVIEW

Intrusion detection systems (IDSs) have become an essential component of network security. IDSs are designed to detect and respond to malicious activities in computer systems and networks. There are two types of IDSs: signature-based and anomaly-based. Signature-based IDSs detect known attacks by comparing network traffic against a database of attack signatures, while anomaly-based IDSs detect unknown attacks by detecting deviations from normal network behavior [77].

In recent years, research has focused on enhancing the accuracy and efficiency of IDSs through the use of machine learning (ML) techniques. ML-IDSs are capable of learning and adapting to new threats without the need for manual signature updates. Researchers have employed a wide range of ML algorithms, including decision trees, neural networks, support vector machines, and ensemble methods, to improve the accuracy and efficiency of IDSs.

Several studies have evaluated the effectiveness of ML-IDSs using the UNSW-NB15 dataset. For instance, Liu et al. (2020) proposed a deep neural-network-based IDS that achieved an accuracy of 99.7% and an F1-score of 0.997. The study by Lazcano et al. (2018) used a hybrid IDS based on a random forest algorithm and achieved an accuracy of 99.1% and an F1-score of 0.989.

In addition to ML techniques, researchers have also explored the use of other methods to improve IDS performance. For instance, several studies have focused on feature selection techniques to reduce the dimensionality of data and improve the accuracy of IDSs. Liu et al. (2019) used a feature selection method based on the Relief algorithm and achieved an accuracy of 99.4% and an F1-score of 0.994 [78].

Furthermore, the use of deep learning techniques, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), has also gained popularity in IDS research. These techniques have been shown to effectively capture temporal and spatial features in network traffic data. For instance, Haddouti et al. (2020) proposed a CNN-based IDS that achieved an accuracy of 99.1% and an F1-score of 0.99, while Huang et al. (2021) proposed an RNN-based IDS that achieved an accuracy of 98.9% and an F1-score of 0.986.

Another area of IDS research is the use of ensemble methods, which combine multiple IDSs to improve the accuracy and robustness of the system. For instance, Liu et al. (2018) proposed an ensemble IDS that combined a decision-tree-based IDS and a random-forest-based IDS, achieving an accuracy of 99.5% and an F1-score of 0.995.

Despite the progress made in IDS research, challenges still need to be addressed. For instance, the lack of labeled data is a major challenge in IDS research. Collecting and labeling large amounts of data is time-consuming and costly, making it difficult to develop and evaluate IDSs. Moreover, IDSs are prone to false positives and false negatives, which can affect the performance of the system.

In conclusion, IDSs are critical for network security, and ML techniques have shown promise in improving the accuracy and efficiency of IDSs. Researchers have employed a wide range of ML algorithms, feature selection techniques, and deep learning techniques to enhance IDS performance. Further research is needed to address the challenges of IDS development and evaluation, such as the lack of labeled data and the issue of false positives and false negatives.

7.7 IDS IN CLOUD COMPUTING ENVIRONMENTS

Intrusion detection systems (IDSs) are critical for securing cloud computing environments due to the multi-tenant nature of the cloud and the potential for the lateral movement of attackers within the cloud. IDSs in cloud computing environments need to handle large volumes of network traffic and be able to detect both external and internal threats. Moreover, IDSs in the cloud need to be able to handle the dynamic nature of cloud computing environments, including auto-scaling, workload migration, and network virtualization. Research has focused on developing IDSs that are specifically designed for cloud computing environments, including IDSs that use virtualization-aware techniques and machine learning algorithms to improve detection accuracy and efficiency [79].

Here are five popular vendors of cloud-based intrusion detection systems (IDSs):

1. **Alert Logic:** Alert Logic is a provider of security-as-a-service solutions, including cloud-based IDS. Their IDS offering, Threat Manager, is designed to detect threats across cloud and hybrid environments.
2. **Trend Micro:** Trend Micro offers a range of cloud security solutions, including their Cloud One–Workload Security platform, which includes IDS capabilities to protect against threats in cloud environments.
3. **Cisco:** Cisco offers a cloud-based IDS solution called Stealthwatch Cloud that uses machine learning and behavior analytics to detect and respond to threats in the cloud.
4. **McAfee:** McAfee’s Cloud Workload Security platform includes IDS capabilities to help detect and prevent attacks on cloud workloads, using a combination of signature-based and behavior-based techniques.
5. **Palo Alto Networks:** Palo Alto Networks offers a cloud-based IDS solution called Prisma Cloud IDS that uses AI-powered threat detection to identify and respond to security threats in cloud environments.

7.8 IDS IN INDUSTRIAL CONTROL SYSTEMS

Here are five popular vendors of intrusion detection systems (IDS) for industrial control systems (ICS) [80]:

1. **Darktrace:** Darktrace offers an AI-based IDS solution specifically designed for ICS environments, called Industrial Immune System. This system uses machine learning algorithms to detect and respond to cyber threats in real time.

2. **Dragos:** Dragos specializes in providing cyber security solutions for ICS environments, including their Dragos Platform, which includes IDS capabilities for detecting and responding to cyber attacks in real time.
3. **Nozomi Networks:** Nozomi Networks provides a range of cyber security solutions for ICS environments, including their Guardian solution, which includes IDS capabilities for detecting and responding to cyber threats in real time.
4. **FireEye:** FireEye offers a range of cyber security solutions, including their Helix platform, which includes IDS capabilities specifically designed for ICS environments.
5. **SecurityMatters:** SecurityMatters provides a range of cyber security solutions for ICS environments, including their SilentDefense platform which includes IDS capabilities for detecting and responding to cyber threats in real time.

7.9 CHALLENGES IN IDS DEVELOPMENT AND EVALUATION

The development and evaluation of intrusion detection systems (IDS) face several challenges that need to be overcome to ensure effective and reliable security. Here are some of the key challenges [81]:

- **Data Quality:** IDSs rely on high-quality data to effectively detect and respond to cyber threats. However, data quality can be affected by various factors, including data incompleteness, inconsistency, and ambiguity. This can impact the accuracy of IDSs, as they may fail to detect threats or may generate false positives.
- **Data Volume:** The volume of data generated in modern networks is often very large, and IDSs need to be able to handle this volume to effectively detect threats. This can require significant processing power, storage, and network bandwidth, which can be challenging to manage.
- **Diversity of Threats:** Cyber threats are constantly evolving and becoming more sophisticated, and IDSs need to be able to detect a wide range of threats, including previously unseen or zero-day attacks. This can require the use of advanced detection techniques and ongoing updates to the IDSs to keep up with new threats.
- **False Positives:** IDSs can generate false positives, which can lead to unnecessary alerts and wasted resources. False positives can be caused by a range of factors, including data quality issues and limitations in the IDS algorithms. Minimizing false positives is essential for effective IDS operation.
- **Integration with Other Security Solutions:** IDSs need to be able to integrate with other security solutions, including firewalls, antivirus software, and security information and event management (SIEM) systems. This can be challenging due to differences in technology and data formats and can impact the effectiveness of the overall security infrastructure.
- **Cost and Complexity:** IDSs can be costly to implement and maintain, particularly for organizations with limited resources. In addition, IDSs can be complex to manage, requiring specialized skills and knowledge to operate effectively.

To address these challenges, researchers and practitioners are exploring various solutions. For example, advances in machine learning and artificial intelligence are being used to improve IDS accuracy and reduce false positives. Cloud-based IDSs are also becoming more common, offering more scalable and cost-effective solutions. The development of standardized evaluation metrics and datasets can also help ensure a more accurate and reliable evaluation of IDSs. Finally, a collaboration between different security vendors and industry groups can help improve the integration of IDSs with other security solutions and address issues related to data quality and the diversity of threats.

7.10 FUTURE DIRECTIONS IN IDS RESEARCH

Intrusion detection systems (IDS) research has made significant progress in recent years, but there are still many challenges and opportunities for further development. Here are some future directions in IDS research:

- **Machine Learning and Artificial Intelligence:** Machine learning and artificial intelligence have the potential to significantly improve IDS accuracy and to reduce false positives. Research in this area is focused on developing new algorithms that can effectively detect and respond to cyber threats in real time.
- **Big Data Analytics:** With the increasing volume of data generated in modern networks, big data analytics is becoming an important area of IDS research. Research is focused on developing new techniques for processing, analyzing, and visualizing large-scale network data to improve IDS effectiveness.
- **Cloud-Based IDS:** Cloud-based IDSs are becoming more popular due to their scalability, cost-effectiveness, and ease of deployment. Future research is focused on improving the performance and reliability of cloud-based IDSs and developing new models for IDS as a service.
- **IoT and Mobile IDS:** The growing use of IoT devices and mobile devices presents new challenges for IDSs, including the need to handle large volumes of data and to support real-time detection and response. Future research is focused on developing new IDS techniques and models that can effectively detect and respond to threats in these environments.
- **Automated Response:** Automated response systems can help reduce the time to detect and respond to cyber threats, and can improve overall security posture. Future research is focused on developing new models and techniques for automated response and integrating these systems with IDSs to create more effective security solutions.
- **Adversarial Machine Learning:** Adversarial machine learning techniques can be used to generate attacks that are specifically designed to evade IDSs. Future research is focused on developing new IDS models and techniques that can effectively detect and respond to these types of attacks.
- **Blockchain-Based IDS:** Blockchain technology has the potential to create more secure and decentralized IDSs. Future research is focused on developing new models and techniques for blockchain-based IDSs that can effectively detect and respond to cyber threats.

7.11 CONCLUSION

Intrusion detection systems (IDSs) play a critical role in modern cyber security, helping organizations detect and respond to cyber threats in real time. IDSs are constantly evolving to keep up with new and emerging threats and to provide more accurate and effective detection and response capabilities.

Recent advances in machine learning, big data analytics, cloud computing, and other technologies have significantly improved IDS effectiveness and scalability. However, there are still many challenges and opportunities for further research and development.

Future research in IDS is focused on developing more accurate, effective, and scalable systems that can effectively detect and respond to cyber threats in real time and that can be integrated with other security solutions to create more comprehensive security infrastructures. Advancements in machine learning, big data analytics, cloud computing, IoT, and blockchain are expected to play a significant role in shaping the future of IDS research and development.

Overall, IDSs are a critical component of modern cyber security, helping organizations protect their networks, data, and assets from cyber threats. As threats continue to evolve, IDSs will continue to evolve, helping organizations stay ahead of the curve and maintain effective security postures.

REFERENCES

- [1]. M. Sabahi-Kaviani and M. Salehi, "Intrusion detection system in cloud computing: A comprehensive review," *Journal of Network and Computer Applications*, vol. 103, pp. 1–22, 2018.
- [2]. S. Jha and S. S. Iyengar, "Intrusion detection system using data mining techniques: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
- [3]. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the Military Communications and Information Systems Conference (MilCIS)*, IEEE, Canberra, Australia, 2015, pp. 1–6.
- [4]. Y. Xiang and W. Zhou, "Intrusion detection in cloud computing: A survey," *IEEE Access*, vol. 3, pp. 1443–1460, 2015.
- [5]. A. Al-Dhaqm and S. Zeadally, "A survey of intrusion detection systems in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–120, 2014.
- [6]. J. Han, "Data mining methods for improving intrusion detection," in *Proceedings of the International Conference on Data Mining*, IEEE, Orlando, FL, USA, 2002.
- [7]. J. Pang, Y. Liu, and Y. Wang, "Intrusion detection in industrial control systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2676–2685, 2018.
- [8]. R. Khan and M. Al-Muhtadi, "A survey of intrusion detection systems in cloud computing," *International Journal of Computer Applications*, vol. 61, no. 3, pp. 28–38, 2013.
- [9]. H. Ali and M. Qasim, "Intrusion detection system: A comprehensive review," *International Journal of Computer Science and Network Security*, vol. 12, no. 7, pp. 1–7, 2012.
- [10]. K. Zhang, K. Xing, and W. Zhou, "A survey of intrusion detection techniques in cloud computing," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.
- [11]. A. Esmailpour, A. Ardeshircham, and M. Mozaffari-Kermani, "A comprehensive review on intrusion detection systems," *Journal of Network and Computer Applications*, vol. 60, pp. 42–58, 2016.

- [12]. A. Al-Nemrat, "Intrusion detection system: A comprehensive review," *Journal of Computer Science and Technology*, vol. 15, no. 2, pp. 86–105, 2015.
- [13]. Y. Zhang, W. Wang, and X. Yu, "A survey on intrusion detection in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–11, 2013.
- [14]. D. D. Dzung and L. E. Turner, "Intrusion detection in SCADA systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1579–1589, 2013.
- [15]. M. Sabahi-Kaviani and M. Salehi, "Intrusion detection system in cloud computing: A comprehensive review," *Journal of Network and Computer Applications*, vol. 103, pp. 1–22, 2018.
- [16]. S. Jha and S. S. Iyengar, "Intrusion detection system using data mining techniques: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
- [17]. N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proceedings of the Military Communications and Information Systems Conference (MilCIS)*, IEEE, Canberra, Australia, 2015, pp. 1–6.
- [18]. Y. Xiang and W. Zhou, "Intrusion detection in cloud computing: A survey," *IEEE Access*, vol. 3, pp. 1443–1460, 2015.
- [19]. A. Al-Dhaqm and S. Zeadally, "A survey of intrusion detection systems in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–120, 2014.
- [20]. J. Han, "Data mining methods for improving intrusion detection," in *Proceedings of the International Conference on Data Mining*, IEEE, Maebashi City, Japan, 2002.
- [21]. J. Pang, Y. Liu, and Y. Wang, "Intrusion detection in industrial control systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2676–2685, 2018.
- [22]. R. Khan and M. Al-Muhtadi, "A survey of intrusion detection systems in cloud computing," *International Journal of Computer Applications*, vol. 61, no. 3, pp. 28–38, 2013.
- [23]. H. Ali and M. Qasim, "Intrusion detection system: A comprehensive review," *International Journal of Computer Science and Network Security*, vol. 12, no. 7, pp. 1–7, 2012.
- [24]. K. Zhang, K. Xing, and W. Zhou, "A survey of intrusion detection techniques in cloud computing," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.
- [25]. A. Esmaeilpour, A. Ardeshiricham, and M. Mozaffari-Kermani, "A comprehensive review on intrusion detection systems," *Journal of Network and Computer Applications*, vol. 60, pp. 42–58, 2016.
- [26]. A. Al-Nemrat, "Intrusion detection system: A comprehensive review," *Journal of Computer Science and Technology*, vol. 15, no. 2, pp. 86–105, 2015.
- [27]. Y. Zhang, W. Wang, and X. Yu, "A survey on intrusion detection in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–11, 2013.
- [28]. D. D. Dzung and L. E. Turner, "Intrusion detection in SCADA systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1579–1589, 2013.
- [29]. M. Sabahi-Kaviani and M. Salehi, "Intrusion detection system in cloud computing: A comprehensive review," *Journal of Network and Computer Applications*, vol. 103, pp. 1–22, 2018.
- [30]. S. Jha and S. S. Iyengar, "Intrusion detection system using data mining techniques: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
- [31]. L. Zhiqiang, G. Mohi-Ud-Din, L. Bing, L. Jianchao, Z. Ye, and L. Zhijun, "Modeling network intrusion detection system using feed-forward neural network using unsw-nb15 dataset," in *Proc. of 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE)*, IEEE, Oshawa, Ontario, Canada, 2019, pp. 299–303.
- [32]. Y. Xiang and W. Zhou, "Intrusion detection in cloud computing: A survey," *IEEE Access*, vol. 3, pp. 1443–1460, 2015.

- [33]. A. Al-Dhaqm and S. Zeadally, "A survey of intrusion detection systems in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–120, 2014.
- [34]. A. Riaz, H. F. Ahmad, A. Kiani, J. Qadir, R. Rasool, and U. Younis, "Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions," *Journal of Information Science and Engineering*, vol. 33, pp. 611–634, 2017.
- [35]. J. Pang, Y. Liu, and Y. Wang, "Intrusion detection in industrial control systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2676–2685, 2018.
- [36]. R. Khan and M. Al-Muhtadi, "A survey of intrusion detection systems in cloud computing," *International Journal of Computer Applications*, vol. 61, no. 3, pp. 28–38, 2013.
- [37]. H. Ali and M. Qasim, "Intrusion detection system: A comprehensive review," *International Journal of Computer Science and Network Security*, vol. 12, no. 7, pp. 1–7, 2012.
- [38]. K. Zhang, K. Xing, and W. Zhou, "A survey of intrusion detection techniques in cloud computing," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.
- [39]. A. Esmailpour, A. Ardeshircham, and M. Mozaffari-Kermani, "A comprehensive review on intrusion detection systems," *Journal of Network and Computer Applications*, vol. 60, pp. 42–58, 2016.
- [40]. A. Al-Nemrat, "Intrusion detection system: A comprehensive review," *Journal of Computer Science and Technology*, vol. 15, no. 2, pp. 86–105, 2015.
- [41]. Y. Zhang, W. Wang, and X. Yu, "A survey on intrusion detection in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–11, 2013.
- [42]. D. D. Dzung and L. E. Turner, "Intrusion detection in SCADA systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1579–1589, 2013.
- [43]. M. Sabahi-Kaviani and M. Salehi, "Intrusion detection system in cloud computing: A comprehensive review," *Journal of Network and Computer Applications*, vol. 103, pp. 1–22, 2018.
- [44]. S. Jha and S. S. Iyengar, "Intrusion detection system using data mining techniques: A survey," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.
- [45]. A. Mahfouz, A. Abuhussein, D. Venugopal, and S. Shiva, "Ensemble classifiers for network intrusion detection using a novel network attack dataset," *Future Internet*, vol. 12, no. 11, p. 180, 2020.
- [46]. Y. Xiang and W. Zhou, "Intrusion detection in cloud computing: A survey," *IEEE Access*, vol. 3, pp. 1443–1460, 2015.
- [47]. A. Al-Dhaqm and S. Zeadally, "A survey of intrusion detection systems in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 42, pp. 102–120, 2014.
- [48]. Y. Mehmood, M. A. Shibli, U. Habiba, and R. asood, "Intrusion detection system in cloud computing: Challenges and opportunities," In *Proc. of 2013 2nd national conference on information assurance (NCIA)*, IEEE, Rawalpindi, Pakistan, 2013, pp. 59–66.
- [49]. J. Pang, Y. Liu, and Y. Wang, "Intrusion detection in industrial control systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2676–2685, 2018.
- [50]. R. Khan and M. Al-Muhtadi, "A survey of intrusion detection systems in cloud computing," *International Journal of Computer Applications*, vol. 61, no. 3, pp. 28–38, 2013.
- [51]. H. Ali and M. Qasim, "Intrusion detection system: A comprehensive review," *International Journal of Computer Science and Network Security*, vol. 12, no. 7, pp. 1–7, 2012.
- [52]. K. Zhang, K. Xing, and W. Zhou, "A survey of intrusion detection techniques in cloud computing," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013.
- [53]. A. Esmailpour, A. Ardeshircham, and M. Mozaffari-Kermani, "A comprehensive review on intrusion detection systems," *Journal of Network and Computer Applications*, vol. 60, pp. 42–58, 2016.

- [54]. A. Al-Nemrat, "Intrusion detection system: A comprehensive review," *Journal of Computer Science and Technology*, vol. 15, no. 2, pp. 86–105, 2015.
- [55]. Y. Zhang, W. Wang, and X. Yu, "A survey on intrusion detection in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 1–11, 2013.
- [56]. D. D. Dzung and L. E. Turner, "Intrusion detection in SCADA systems: A survey," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1579–1589, 2013.
- [57]. X. Li, Y. Li, and J. Liu, "A hybrid intrusion detection model based on stacked autoencoder and convolutional neural network," in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Rome, Italy, 2017, pp. 288–295.
- [58]. Y. Yao, Q. Zheng, and B. Hu, "Intrusion detection using deep belief networks," in *2016 IEEE 18th International Conference on High-Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, Australia, 2016, pp. 1042–1047.
- [59]. Y. Yao, Q. Zheng, and B. Hu, "An intrusion detection system based on deep learning," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, Canada, 2017, pp. 1722–1727.
- [60]. J. Lin, Z. Hu, Y. Liu, and X. Liu, "Network intrusion detection based on deep belief network," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, Chengdu, China, 2015, pp. 189–194.
- [61]. R. G. Al-Shammari, A. M. Al-Sumait, and A. A. R. Al-Ali, "Intrusion detection using deep learning algorithms," in *2018 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia, 2018, pp. 1–6.
- [62]. J. Wang, Y. Zhang, Y. Sun, and C. Yang, "A deep learning approach for network intrusion detection system," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICT)*, Kannur, India, 2017, pp. 331–335.
- [63]. J. Cai, Z. Li, Y. Liu, H. Xu, and Y. Xu, "Deep learning-based feature representation and its application for intrusion detection," *Journal of Network and Computer Applications*, vol. 107, pp. 107–119, 2018.
- [64]. M. Mahdianpari, H. Dehghantanha, R. Khayami, and A. Karimpour, "Deep learning for intelligent intrusion detection system: A systematic review," *Journal of Information Security and Applications*, vol. 50, pp. 49–69, 2020.
- [65]. T. Nguyen, H. Nguyen, and T. Le, "Intrusion detection system using deep learning and hybrid features," in *2019 5th International Conference on Green Technology and Sustainable Development (GTSD)*, Ho Chi Minh City, Vietnam, 2019, pp. 277–282.
- [66]. Y. Wang, X. Xie, and K. Guan, "Network intrusion detection based on deep learning with one-class classification," in *2018 10th International Conference on Machine Learning and Computing (ICMLC)*, Macau, China, 2018, pp. 290–295.
- [67]. R. A. Sarker, H. S. Kim, and S. H. Kim, "A deep learning-based hybrid intrusion detection system," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 4, pp. 2239–2251, 2018.
- [68]. X. Li, Y. Li, and J. Liu, "A hybrid intrusion detection model based on stacked autoencoder and convolutional neural network," in *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Rome, Italy, 2017, pp. 288–295.
- [69]. Y. Yao, Q. Zheng, and B. Hu, "Intrusion detection using deep belief networks," in *2016 IEEE 18th International Conference on High-Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, Australia, 2016, pp. 1042–1047.

- [70]. Y. Yao, Q. Zheng, and B. Hu, "An intrusion detection system based on deep learning," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, Canada, 2017, pp. 1722–1727.
- [71]. J. Lin, Z. Hu, Y. Liu, and X. Liu, "Network intrusion detection based on deep belief network," in *2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity)*, Chengdu, China, 2015, pp. 189–194.
- [72]. R. G. Al-Shammari, A. M. Al-Sumait, and A. A. R. Al-Ali, "Intrusion detection using deep learning algorithms," in *2018 International Conference on Advanced Technologies for Signal and Image Processing (ATSIP)*, Sousse, Tunisia, 2018, pp. 1–6.
- [73]. J. Wang, Y. Zhang, Y. Sun, and C. Yang, "A deep learning approach for network intrusion detection system," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Kannur, India, 2017, pp. 331–335.
- [74]. J. Cai, Z. Li, Y. Liu, H. Xu, and Y. Xu, "Deep learning-based feature representation and its application for intrusion detection," *Journal of Network and Computer Applications*, vol. 107, pp. 107–119, 2018.
- [75]. M. Mahdianpari, H. Dehghantanha, R. Khayami, and A. Karimipour, "Deep learning for intelligent intrusion detection system: A systematic review," *Journal of Information Security and Applications*, vol. 50, pp. 49–69, 2020.
- [76]. T. Nguyen, H. Nguyen, and T. Le, "Intrusion detection system using deep learning and hybrid features," in *2019 5th International Conference on Green Technology and Sustainable Development (GTSD)*, Ho Chi Minh City, Vietnam, 2019, pp. 277–282.
- [77]. Zhao, Chengying, Xianzhen Huang, Yuxiong Li, and Muhammad Yousaf Iqbal. 2020. "A double-channel hybrid deep neural network based on CNN and BiLSTM for remaining useful life prediction," *Sensors* 20, no. 24: 7109. <https://doi.org/10.3390/s20247109>
- [78]. Liu, Hongyu and Bo Lang. 2019. "Machine learning and deep learning methods for intrusion detection systems: A survey," *Applied Sciences*, vol. 9, no. 20, p. 4396. <https://doi.org/10.3390/app9204396>
- [79]. Y. Wang, X. Xie, and K. Guan, "Network intrusion detection based on deep learning with one-class classification," in *2018 10th International Conference on Machine Learning and Computing (ICMLC)*, Macau, China, 2018, pp. 290–295.
- [80]. R. A. Sarker, H. S. Kim, and S. H. Kim, "A deep learning-based hybrid intrusion detection system," *Journal of Intelligent & Fuzzy Systems*, vol. 34, no. 4, pp. 2239–2251, 2018.
- [81]. A. Abbas, M.A. Khan, S. Latif, et al., "A new ensemble-based intrusion detection system for internet of things," *Arabian Journal for Science and Engineering*, vol. 47, pp. 1805–1819, 2022. <https://doi.org/10.1007/s13369-021-06086-5>

8 Signature-Based Intrusion Detection System for IoT

Bakhtawar Nawaal, Usman Haider, Inam Ullah Khan, and Muhammad Fayaz

8.1 INTRODUCTION

The Internet of Things (IoT) is a network of devices that communicates over the Internet and distributes information among themselves and the external environment. The term IoT was first used by Kevin Ashton in 1998 when he mentioned that the IoT has the potential to change the entire world. It has improved people's lifestyle by adding intelligent systems to our environments. Evolution in IoT has added billions of IoT devices to the Internet. Its applications have progressed in diverse streams including fitness, health, automation, and smart societies [1]. With IoT technologies, cities have become more efficient. Traffic is managed smartly using sensors. Smart parking has saved fuel and time for drivers by providing data on available slots. Smart waste management, street lights, water supply, environment, etc. have effectively enhanced the lifestyle of citizens. Smart farming has helped thousands of farmers in managing the requirements of water, fertilizer, and manure for plants. The quality of human life has improved too with effective healthcare systems that monitor the patient's health and track changes [2].

Increasing demand for devices has provided space for various attacks from worms, viruses, Trojan horses, malware, etc. [3]. With time, devices have become more vulnerable to security attacks. Commonly encountered attack includes DoS and DDoS. A denial-of-service (DoS) attack tends to shut down network resources for the host [4]. In a distributed denial-of-service (DDoS) attack, the attacker utilizes resources from multiple locations to affect the network. According to a Cisco white paper, DDoS attacks will reach total 15 million by 2023, compared to 7 million in 2018 [5]. IoT botnets have posed a great danger to IoT devices. The most common examples of botnets include Linux/Hydra, Psyb0t, Linuz Darlloz, Spike (Dofloo), BASHLITE, Mirai, etc. [6]. Other types of attacks include brute force attacks, rolling code attacks, BlueBorne attacks, Sybil attacks, and buffer overflow attacks, all of which affect IoT components. Sybil attacks use fabricated devices to hinder the performance of network devices and create traffic junctions [7]. The BlueBorne virus attacks the device via Bluetooth and involves no human interaction [8]. List of attacks keeps on increasing with the addition of devices on Internet.

Ultimately these consequences of cyber attacks have led to the major development of intrusion detection system (IDS) and intrusion prevention system (IPS). An IDS provides extensive surveillance, which detects unusual or malicious traffic entering the network [9]. Three basic genres of IDS are:

- 1. Signature-based IDS.
- 2. Anomaly-based IDS.
- 3. Hybrid-based IDS.

A signature-based IDS consists of existing patterns of malicious codes that are utilized in identifying attacks. This IDS is easy to use. An anomaly-based IDS compares data patterns with already created data of normal behavior of packets to detect abnormality [10]. A hybrid-based IDS is the union of both of the later types; hence it lowers the error rate. It can detect multiple categories of attacks from a variety of reckoning environments. An overview of signature-based intrusion detection is shown in Figure 8.1.

Signature-based ID systems depend on previously defined attacks and is better than anomaly-based in certain ways. It is simple and operates online in real time [11]. It observes certain patterns and events and matches them with signatures

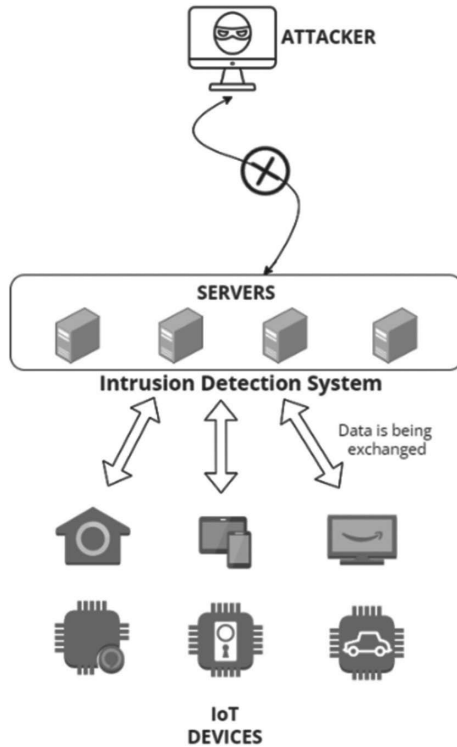


FIGURE 8.1 Overview of signature-based IDS.

of attacks on a predefined list of known indicators of compromise (IOCs). Eighty percent of incidents in any cyber physical system are easily marked and detected using signature-based methodologies [12].

8.2 LITERATURE STUDY

This section discusses the recent work performed to extract limitations related to intrusion detection systems using various techniques.

Intrusion detection systems functions on a certain algorithm. There has been plenty of work related to various IDSs previously, which has helped in delivering important outcomes. To identify selective forwarding black hole attacks, Hidoussi et al. [13] presented a signature-based IDS. It was meant for wireless sensor networks (WSNs) that are cluster based. Another signature-based IDS was proposed by Patel SK et al. [14] to identify port scan attacks via (EPSDR), which is port scan detection rule. Mehare et al. [15] designed an IoT-based IDS that depended on the location and neighborhood information of the nodes that were attacked. This paper covered only the DoS attack and did not evaluate the proposed model in the paper. Krimmling et al. [16] suggested a signature-based IDS that worked on ML algorithms. The system uses a lightweight algorithm and is applied to CoAP applications. Liu et al. [17] established an artificial immune IDS for an IoT environment. The IDS could learn new attacks, which are based on ML and signature-based models.

A unified intrusion detection system (UIDS) was suggested by Kumar et al. [18] for IoT-based networks. The model was analyzed on the upgraded dataset UNSW-NB15. An analysis of the UNSW-NB15 [19] dataset was directed by Moustafa et al. [14]. They compared the operation of this dataset with KDD99 [20] using machine learning. Koroniotis et al. [21] also conducted an analysis of various ML techniques using the UNSW-NB15 dataset to check how it detects intrusions in the network. Garcia-Font et al. [22] suggested an IDS for wireless sensor networks (WSNs) using a signature-based approach and ML techniques. They improved the detection rate and FPR by using a signature and anomaly-based detection engines. The main goal of the system is to identify malicious codes in WSNs in various smart city environments and was also applicable to large city environments.

Various types of IDSs have certain limitations. Anomaly-based IDSs depend on the statistical features of normal traffic and can identify unknown attacks. Major issues encountered by these systems are the high false-positive ratio when it comes to unpredictable traffic [23]. It also causes problems while processing and analyzing big data [24]. Utilization of outdated datasets has also caused hindrances in evaluating the performance of IDS [25]. Labeling of datasets is another hurdle faced if it is not done rightly. The correct labeling of datasets makes the IDS reliable by defining all attacks [26]. Moreover, labeling improves the accuracy of detection by making use of supervised learning algorithms [27].

Signature-based IDS also encounters problems in detecting polymorphic worms and metamorphic malware due to the rewriting process in every iteration. Polymorphic worms are the greatest challenge for signatures-based IDS as they modify and replicate themselves to fool the system. However, Y-Tang and S. Chen proposed an intrusion detection system that could detect polymorphic worms via

position-aware distribution signatures. (PADS) [24]. A signature-based IDS detects already known attacks through a database of patterns [28]. Some of its disadvantages include false alarms, overloading of network packets, and high cost of signature matching [29]. Memory constraints also pose some disadvantages to the signature-based system by making it less performant due to the storage of huge databases [30]. Pattern databases in a signature-based IDS need to be consistently changed. These IDSs detect intrusions based on previous knowledge. Table 8.1 shows the limitations of various types of IDSs.

TABLE 8.1
Limitations of IDSs

Reference	Type of IDS	Technique Used	Behavior	Description	Limitations
[31]	Signature-based	Pattern matching approach	Depends on preexisting patterns of malicious codes.	Proposed a pattern-matching IDS for embedded security systems. It uses an auxiliary skipping (AS) algorithm, which helps in reducing the number of matching operations. This IDS applies to smart objects that have confined memory size.	Does not allow finding higher-order pattern malware.
[32]	Anomaly-based	Machine learning	Compares normal traffic with current incoming data packets.	IDS uses a mathematical algorithm to train itself on normal dataset. It learns characteristics and then detects the malicious codes.	Takes long time in training data and identifies threats from alerts.
[33]	Anomaly-based	Machine learning	The IDS captures human activity or inactivity through IoT device sensors placed in the simulated smart environment.	This IDS uses machine learning technique that is based on an artificial immune system. It is a behavior modeling IDS that decides whether the behavior is acceptable or not.	Vague warning leads to the provision of unclear information to the administrator.
[34]	Hybrid-based	DT, SVM algorithms	The ensemble approach gave better results.	This work presented the use of machine learning through decision tree (DT) and support vector machine (SVM) techniques for efficient IDS.	SVM does not satisfy in the case of larger datasets.

TABLE 8.1 (Continued)
Limitations of IDSs

Reference	Type of IDS	Technique Used	Behavior	Description	Limitations
[35]	Hybrid-based	Deep neural network (DNN)	Significantly flexible on commodity hardware server	This paper proposed the use of deep learning to counter the problems of high false alarm rate, single dataset usage, and modern huge network obstinacy.	The details regarding the malware cannot be acquired using this model.
[36]	Anomaly-based	Naïve Bayes (NB)	A threshold is defined to differentiate between the normal and attack records.	This work presented an IDS based on Bayesian probability using KDD dataset and NB classifier.	The NB classifier has limited functionality in real time.
[37]	Hybrid-based	Convolutional neural network (CNN)	The model works in four stages, i.e., data collection, preprocessing, training, and detection.	This paper proposed an IDS based on CNN for the IoT environment and network, divided into various layers, i.e., convolutional, input, and hidden layers.	CNN model is comparatively slower.
[38]	Signature-based	Hybrid placement strategy	The proposed used an IDS border router (BR) and various detectors in IoT network.	This research suggested a new signature-based IDS for IoT framework. It incriminates centralized and distributed IDS modules.	Zero-day exploit remains unattended.
[39]	Signature-based	Collaborative blockchain technology	The model is divided in various nodes, and IDS nodes exchange data with each other.	The work suggested a blockchain-based IDS, CBSigIDS for IoT habitat by integrating the blockchains with distributed signature-based IDS.	The system's accuracy needs improvement, and blockchain technology can be vulnerable to various attacks.

8.3 SECURITY CHALLENGES AND CYBER ATTACKS IN THE IOT NETWORK

All devices in an IoT system communicate wirelessly, and therefore they are exposed to several vulnerabilities that bridge all layers of the IoT architecture. It must be prevented from threats [40]. Compatibility and complexity are the two most significant challenges that IoT-based environments face. They are mostly affected

TABLE 8.2
Categories of Security Challenges Faced by IoT Systems

Sr. No.	Categories	Detail
1	Validation and vulnerabilities	Mostly perceived by sensors as they are open to physical attacks
2	Confidentiality compromises	Occurs between network layer and gateways
3	Data integrity inconsistencies	Arises during applications and service of IT systems, when IoT system is affected by noise or attack
4	Privacy violations	Data privacy is the most important challenge faced by IoT systems.

by denial-of-service (DoS), distributed denial-of-service (DDoS), SQL injection attacks, ping of death (PoD) attacks, sinkhole attacks, etc. [41]. A sinkhole attack is launched by an inside attacker, whereas a DoS attack makes the network unavailable to the users. IoT systems face four types of security issues:

1. Validation and vulnerabilities
2. Confidentiality compromises
3. Data integrity inconsistencies
4. Privacy violations

Table 8.2 describes the cyber issues that are commonly raised in different IoT layers [42].

The utilization of various technologies and products in the IoT framework poses threats to the security of smart environments. This is due to a lack of standardization. Moreover, the penetration of a single-end device also causes harm to the whole network [43].

8.4 INTRUSION DETECTION SYSTEM FOR IOT NETWORKS

An intrusion detection system working in an IoT system protects the network from intrusions and threats. It maintains the integrity, availability and confidentiality of the network [44]. IDS detects the network condition and it alerts in the form of alarms. There are four situations of IDS alerts i.e., true positive, true negative, false positive and false negative pointing to real threat, normal scenario, false alert and misdetection respectively [45, 46]. Figure 8.2 explains the classification of threat alerts in IDS.

Two main types of IDSs can be implemented in the system: host-based intrusion detection system (HIDS) and network-based intrusion detection system (NIDS). The HIDS is deployed on a single system and uses the metrics of the host environment to detect attacks [47]. A NIDS senses intrusions from network data packets [48]. Figure 8.3 shows the overview and placement of HIDS and NIDS.





	Positive	Negative
True	 True Positive	 True Negative
False	 False Positive	 False Negative

FIGURE 8.2 Classification of threat alerts.

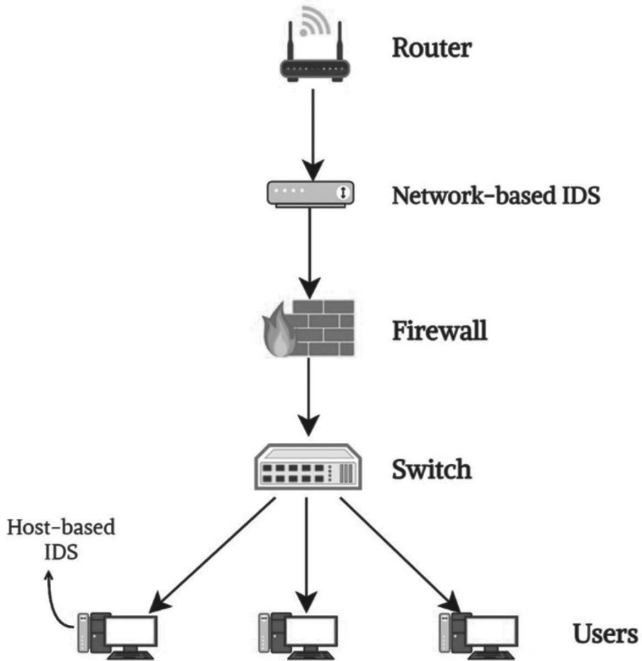


FIGURE 8.3 Overview and placement of HIDS and NIDS.

These two types of IDSs are further classified on the bases of their detection techniques: anomaly-based detection, signature-based detection, and hybrid-based detection.

8.4.1 ANOMALY-BASED IDS FOR IOT

Anomaly-based IDS senses attacks by detecting unusual behaviors in IoT environments [49]. An anomaly signifies abnormal actions in data patterns [50]. The IDS comprises a model that shows the normal expression of data. It is then compared with the patterns of the current data. If deviations occur, then the attack is detected in the environment [51]. Anomaly-based IDS techniques are further classified into several approaches. The data mining approach is applied to large data resources to extract knowledge from them in the form of patterns that describe the behavior of data in the IoT environment [52]. In a statistical approach, the model is created by using historical user data to detect any change. Statistical mathematical operations are applied in this technique to train datasets to capture anomalies [53].

8.4.2 SIGNATURE-BASED IDS FOR IOT

A signature-based technique uses patterns and signatures of known malicious codes to detect attacks [54]. It uses previous knowledge to detect these attacks. Hence, databases of patterns and signatures need to be updated. Writing signatures require expertise as new types of attacks are continuously being discovered. For this, we need to have enough data for analysis purposes and a good understanding of the behavior of signatures [55]. The signature-based technique minimizes false alarms providing accuracy. Hence, many commercial systems are installed with signature-based detection due to the production of fewer false alarms [56]. However, advancement in technology has hindered the efficiency of signature-based IDSs as the number of signatures would also be increased with technologies such as encrypted data channels, NOP generators, and payload encoders [57]. Figure 8.4 explains the concept of signature-based IDS.

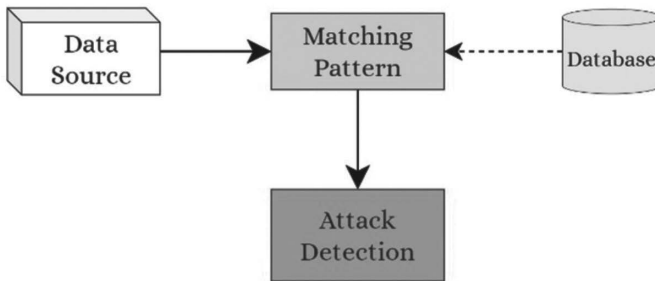


FIGURE 8.4 Concept of signature-based IDS.

8.4.3 HYBRID-BASED IDS FOR IOT

In the hybrid intrusion detection technique, the concept of both HIDS and NIDS is used. It collects data from the host as well as from the network and then analyses it for intrusions. The analysis is held based on anomaly detection or a database of signature-based patterns [58]. Hybrid intrusion detection includes two steps. In the first step, the anomaly detection part of HIDS functions to identify abnormalities using a particular approach. In case of any malicious code identification, its pattern is stored in the signature database to protect the IoT system from similar attacks. This process is executed in the second stage [59]. The hybrid-based IDS accomplishes the targets of a high alarm probability and low false positives [60].

8.5 MACHINE-LEARNING-BASED SIGNATURE IDS SOLUTIONS FOR IOT

Signature-based IDS can be implemented using various machine learning (ML) techniques. The machine learning technique consists of the training and testing stages [61]. During training of a dataset, algorithms use data at the normal state as the information source to train themselves on the features of the IoT network. Thereafter, classification is performed in the testing stage [62]. Some of the ML techniques that can be used to implement signature-based IDS for IoT are discussed next.

In *supervised learning*, the classification model is created by using the characteristics of the training datasets. This is the learning phase of the model [63]. The unsupervised learning model doesn't use clustered training data.

Naïve Bayes algorithm can be used for probability calculations, using network traffic characteristics in a signature-IDS based on an IoT system [64]. Naïve Bayes requires a lower amount of data in the characterization cycle to find the estimated boundaries. It performs well on KDD CUP 1999+NSL and UNSW-NB15 datasets and helps in detecting DDoS, DoS, Code injection, etc. [65].

The *decision tree (DT)* classifier facilitates decision making by using the techniques of information gain and genii index. Data can be manipulated, and missing values can be found by using this algorithm [66]. Decision trees are easy to use and can be implemented to the CICIDS 2017, BOT-IoT, KDD99, NSL-KDD datasets in identifying attacks such as Sybil, flooding, spyware, etc. [67].

K-nearest neighbor (K-NN) calculates the distance between the neighbors using Euclidean distance [68]. *K-NN* categorizes the new occurrence based on the maximum number of nearest neighbors. It can be implemented on datasets such as DS2OS, UNSW-NB15, etc. [69].

Support vector machine (SVM) is another ML technique that helps in real-time detection of both known and unknown attacks [70]. SVM classifies linearly separable data into two-dimensional planes. The kernel function in SVM converts nonlinear data into linear form for attack detection. The performance of SVM depends on the dataset and its environment [71]. Datasets such as UNSW-NB15, KDDCUP99,

NSL-KDD, and NOT-IoT can be used for SVM in detecting attacks like man-in-the-middle attacks, DoS, DDoS, tempering etc. [72].

8.6 DEEP-LEARNING-BASED SIGNATURE-IDS SOLUTIONS FOR IOT

We apply deep learning (DL) techniques while dealing with larger datasets rather than machine-learning-based solutions. These methodologies are widely applied in IDSs. Deep learning is the domain of ML consisting of neural networks that help in finding high-level features of data through layers of modification [73]. In an intrusion detection system, the hidden layers of the neural network help in identifying the best features for pattern selection. It contains an input layer, hidden layer(s) and an output layer. Specific weights are associated with every input of the network, which are adjusted to get the best output via the backpropagation method [74]. Deep learning detection techniques are classified into three main streams: supervised learning, unsupervised learning techniques, and hybrid methods [75].

Some of the famous DL techniques like deep neural networks (DNN), convolutional neural networks (CNN), recurrent neural networks (RNN), etc. are included in supervised learning methods. These methods provide high accuracy. Deep neural networks (DNN) contain numerous hidden layers that aid in feature extraction. Complex functions with fewer parameters can be expressed through these hidden layers. Tang et al. [76] designed a simple DNN that performed flow-based detection. Convolutional neural network (CNN) performs convolution, pooling, full connection with the dataset input. CNN involves less preprocessing. Kolosnjaji et al. [77] designed a model to detect malware by proposing CNN with recursive network layers. Recurrent neural network (RNN) is comprised of a memory function that stores previous data. It efficiently deals with time series information. C. Yin et al. [78] evaluated RNN with binary classification and multiclass classification.

Unsupervised learning techniques include generative adversarial networks (GANs), autoencoder (AE), deep belief networks (DBN), etc. These methods are low in performance as insufficient knowledge is available from labeled data. Gao et al. [79] tried various DBN models to construct an IDS. The best performance was acquired on the KDDCup 99 dataset. The generative adversarial network (GAN) is a type of unsupervised learning that helps to process, scrutinize, and capture data. It consists of a generator and discriminator, which helps in identifying real images from fake ones. Erpek et al. [80] designed a jamming attacks detection model-based on a generative adversarial network consisting of transmitter, receiver, jammer. Autoencoder is a data compression algorithm used for reducing dimensions and detecting outliers. It uses feature space for compressing the input. Zhang et al. [81] proposed an IDS by involving dilated convolutional AE (DCAEs) to extract useful features from original data traffic of network.

Hybrid methods result in high performance and a smaller number of training samples, but computing time is high because of the complex structure. Li et al. [82]

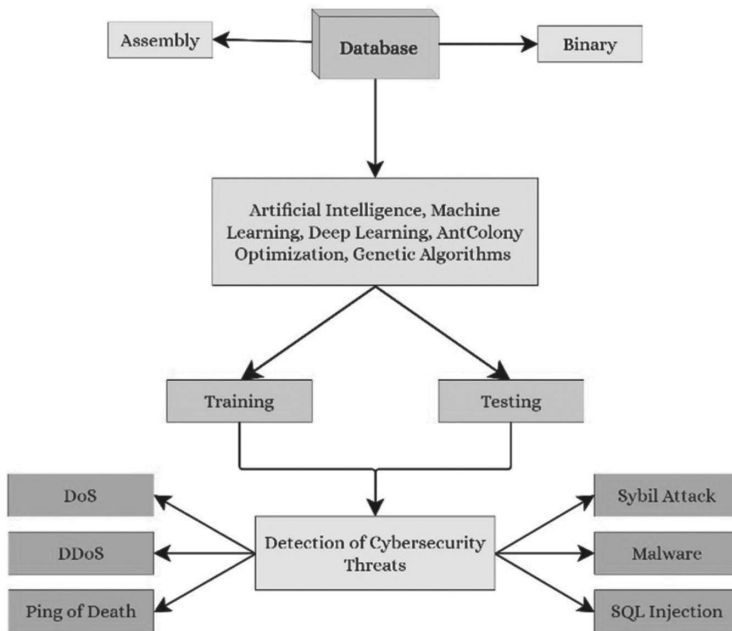


FIGURE 8.5 Threat detection using signature-based IDS.

used a hybrid deep learning technique that implemented autoencoder and deep neural network for anomaly detection. AE was used to reduce the dimensions of data.

8.7 SIGNATURE-BASED INTRUSION DETECTION SYSTEM ARCHITECTURE

Researchers have used various kinds of IDS depending on the framework of the network as well as per requirements. Sourour et al. [83] suggested a two-layered IDS to address the security concerns related to network address translation (NAT). Layer 1 monitors the network entities, and layer 2 is deployed using three modules—alert consolidation, alert classification, and alert correlation—to lower the number of alerts and to pin down false alarms. Yichi Zhang, et al. [84] introduced a dispersive kind of IDS for the smart grid having multilayered architecture using SVM for classification of the attack and clonal selection classification (CSC) algorithm for attack detection. A modular deep learning (MDL) model was also suggested to deploy in an IDS as it has a multi-architectural topology inspired by the human brain, but this concept is still newborn [85]. The application layer is vulnerable to various kinds of attacks, so for cloud security, a signature-based cloud IDS is an efficient approach, thus securing the application layer along with rest of the layers [86, 87]. The common organization and threat detection phenomenon of signature-based IDS is shown in Figure 8.5.

8.8 LIMITATIONS IN SIGNATURE-BASED INTRUSION DETECTION SYSTEM

the signature-based technique for IDS is a widely used approach because it usually has a low false alarm rate and very efficient results. But this technique has some limitations that need to be addressed with proper solutions. Signature-based IDS can only identify the threats whose attack signatures are been saved already; thus it fails to detect anything absent from the database [88], and zero-day-exploit remains unattended [89, 90]. Sometimes it causes a network packet overload, and it has a huge false alarm rate when operated in a large-scale network environment [91]. Each packet in signature-based approach needs to be match examined, in the case that large incoming traffic anomalies occur. In most cases, the following scenario leads to packet drop when the IDS can't handle the traffic, leaving the system open to the chance of missing potential threats [92]. Thus these limitations are termed design or implementation flaws of the signature-based technique [93].

8.9 DISCUSSION AND FUTURE DIRECTIONS

Advances in technology and the Internet of Things have caused great vulnerability to the security of data [94, 95]. Signature-based IDSs are among the most widely installed IDSs in the commercial sector networks due to their pattern-based anomaly detection capability. These systems are improving every day to meet the complexity of new threat variants. A detailed survey of the signature-based IDS, along with various implementation techniques, was discussed in this chapter. Future work can be performed by implementing signature-IDS with specific techniques that make it threat prone and performant. Software such as SNORT, WINPCAP, etc. can be focused on real-time detection and efficiency [96]. Markov distribution also helps in packet filtering in IDS [97]. Furthermore, various DL algorithms can be used to reduce the computational complexity of the IDS as there is huge scope for this, and enormous work can be done in this field.

8.10 CONCLUSION

Security has no longer been a choice in IT infrastructure; it is an utter compulsion to be focused on. The mushroom growth of IoT devices has posed the challenge of security in the IoT environment. Signature-based IDS is an excellent approach to counter security threats. Many solutions using signature-based detection techniques have been suggested by different researchers using different methodologies. The pattern matching approach has been the identification of this type of detection, but it has some limitations leading to false negative conditions and potential danger. The machine learning and deep learning algorithm counters the limitation of signature-based detection by means of training over various datasets, thus decreasing the false detection rate and improving accuracy. This work offers a detailed survey of a variety of signature-based IDSs and the techniques deployed with them by different researchers.

REFERENCES

- [1] Alqahtani B, AlNajrani B (Oct. 2020) A study of Internet of Things protocols and communication. In: *Proceedings of the 2nd International Conference on Computer and Information Sciences (ICCIS)*, pp. 1–6, doi:10.1109/ICCIS49240.2020.9257652.
- [2] Soumyalatha N, Hegde SG (2016) Study of IoT: Understanding IoT architecture, applications, issues and challenges. In: *1st International Conference on Innovations in Computing & Net-working (ICICN16)*, CSE, RRCE, *International Journal of Advanced Networking & Applications*, vol. 478.
- [3] Abdalgawad N, Sajun A, Kaddoura Y, Zualkernan IA, Aloul F (2022) Generative deep learning to detect cyberattacks for the IoT-23 dataset. *IEEE Access* 10: 6430–6441, doi:10.1109/ACCESS.2021.3140015.
- [4] Mann P, Tyagi N, Gautam S, Rana A (2020) Classification of various types of attacks in IoT environment. In: *2020 12th International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE, Bhimtal, India.
- [5] *Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper*. Accessed: May 31, 2021 [Online]. Available: www.cisco.com/c/en/us/solutions/collateral/executiveperspectives/annual-internet-report/white-paper-c11-741490.html.
- [6] Ashraf J, Bakhshi AD, Moustafa N, Khurshid H, Javed A, Beheshti A (2021) Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 22(7): 4507.
- [7] Archana MB, Harshitha BN, Prajakta M (2017) A technique to safeguard cluster-based wireless sensor networks against Sybil attack. *International Journal of Recent Trends in Engineering and Research*, 3(4): 370–373, doi:10.23883/ijrter.2017.3159.jsizq.
- [8] Wang W, He S, Sun L, Jiang T, Zhang Q (2019) Cross technology communications for heterogeneous IoT devices through artificial doppler shifts. *IEEE Transactions on Wireless Communications*, 18(2): 796–806, doi:10.1109/twc.2018.2883443.
- [9] Kumar V (2012) Signature based intrusion detection system using SNORT. *International Journal of Computer Applications & Information Technology*, 1(7).
- [10] Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys and Tutorials*, 16(1): 303–336.
- [11] Tang Y, Chen S (July 2007) An automated signature-based approach against polymorphic internet worms. *IEEE Transactions on Parallel and Distributed Systems*, 18(7): 879–892, doi:10.1109/TPDS.2007.1050.
- [12] Snehi J, Bhandari A, Baggan V, Snehi M (2020) Diverse methods for signature-based intrusion detection schemes adopted. *International Journal of Recent Technology and Engineering*, 9(2): 44–49.
- [13] Hidoussi F, Toral-Cruz H, Boubiche DE, Lakhtaria K, Mihovska A, Voznak M (2015) Centralized IDS based on misuse detection for cluster-based wireless sensors networks. *Wireless Personal Communications*, 85(1): 207–224.
- [14] Patel SK, Sonker A (2016) Rule-based network intrusion detection system for port scanning with efficient port scan detection rules using snort. *International Journal of Future Generation Communication and Networking*, 9(6): 339–350.
- [15] Mehare TM, Bhosale S (2017) Design and development of intrusion detection system for internet of things. *The International Journal of Innovative Research in Computer and Communication Engineering*, 5(7): 13469–13475.

- [16] Krimmling J, Peter S (2014) Integration and evaluation of intrusion detection for CoAP in smart city applications. In: *2014 IEEE Conference on Communications and Network Security*. IEEE, San Francisco, pp. 73–78.
- [17] Liu C, Yang J, Chen R, Zhang Y, Zeng J (2011) Research on immunity-based intrusion detection technology for the internet of things. In: *2011 Seventh International Conference on Natural Computation*, vol. 1. IEEE, Shanghai, pp. 212–216.
- [18] Kumar V, Das AK, Sinha D (2021) UIDS: A unified intrusion detection system for IoT environment. *Evolutionary Intelligence*, 14: 47–59, doi:10.1007/s12065-019-00291-w.
- [19] Mohammadi M, Akbari A, Raaheemi B, Nassersharif B, Asgharian H (2014) A fast anomaly detection system using probabilistic artificial immune algorithm capable of learning new attacks. *Evolutionary Intelligence*, 6(3): 135–156.
- [20] Jha J, Ragha L (2013) Intrusion detection system using support vector machine. In: *International Journal of Applied Information Systems: Proceedings on International Conference and workshop on Advanced Computing ICWAC*, vol 3. Foundation of Computer Science, New York, pp. 25–30.
- [21] Koroniotis N, Moustafa N, Sitnikova E, Slay J (2017) Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. In: *International Conference on Mobile Networks and Management*. Springer, Cham, pp. 30–44.
- [22] Garcia-Font V, Garrigues C, Rifà-Pous H (2017) Attack classification schema for smart city WSNs. *Sensors*, 17(4): 1–24.
- [23] Mitchell R, Chen I-R (2014) A survey of intrusion detection in wireless network applications. *Computer Communications*, 42: 1–23.
- [24] Tang Y, Chen S (July 2007) An automated signature-based approach against polymorphic internet worms. *IEEE Transactions on Parallel and Distributed Systems*, 18(7): 879–892, doi:10.1109/TPDS.2007.1050.
- [25] Moustafa N, Slay J (2015) UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: *Proceedings of the Military Communications and Information Systems Conference (MilCIS)*. IEEE, Canberra, ACT, Australia, pp. 1–6.
- [26] Gogoi P, Bhuyan MH, Bhattacharyya DK, Kalita JK (2012) Packet and flow based network intrusion dataset. In: *Contemporary Computing*, M Parashar, D Kaushik, OF Rana, R Samtaney, Y Yang, and A Zomaya, Eds. Springer, Heidelberg, Germany, pp. 322–334.
- [27] Laskov P, Düssel P, Schäfer C, Rieck K (2005) Learning intrusion detection: Supervised or unsupervised? In: *Image Analysis and Processing (ICIAP)*, F Roli and S Vitulano, Eds. Springer, Heidelberg, Germany, pp. 50–57.
- [28] Bul’ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality-of-service configuration and parallel technology. *Journal of Computer and System Sciences*, 81(6): 981–999.
- [29] Meng W, Li W, Kwok L-F (2014) EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. *Computers & Security*, 43: 189–204.
- [30] Abduvaliyev A, Pathan ASK, Zhou J, Roman R, Wong WC (2013) On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys and Tutorials*, 15(3): 1223–1237.
- [31] Oh D, Kim D, Ro WW (2014) A malicious pattern detection engine for embedded security systems in the internet of things. *Sensors*, 14(12): 24188–24211.
- [32] Elrawy M, Awad A, Hamed H (2018) Intrusion detection systems for IoT-based smart environments: A survey. *Journal of Cloud Computing*, 7(21), doi:10.1186/s13677-018-0123-6.

- [33] Arrington B, Barnett L, Rufus R, Esterline A (2016) Behavioral modeling intrusion detection system (BMIDS) using internet of things (IoT) behavior-based anomaly detection via immunity-inspired algorithms. In: *2016 25th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, Waikoloa, pp. 1–6.
- [34] Peddabachigari S, et al. (2007) Modeling intrusion detection system using hybrid intelligent systems. *Journal of Network and Computer Applications*, 30(1): 114–132.
- [35] Vinayakumar R, et al. (2019) Deep learning approach for intelligent intrusion detection system. *IEEE Access*, 7: 41525–41550.
- [36] Altwaijry H. (2013) Bayesian based intrusion detection system. In: *IAENG Transactions on Engineering Technologies: Special Edition of the World Congress on Engineering and Computer Science 2011*. Springer, San Francisco, USA.
- [37] Smys S, Basar A, Wang H (2020) Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, 2(4): 190–199.
- [38] Ioulianou P, et al. (2018) A signature-based intrusion detection system for the internet of things. In: *Information and Communication Technology Forum*. Graz, Austria, 11–13 July 2018.
- [39] Li W, et al. (2019) Designing collaborative blockchained signature-based intrusion detection in IoT environments. *Future Generation Computer Systems*, 96: 481–489.
- [40] Bandyopadhyay D, Sen J (2011) Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, 58(1): 49–69.
- [41] Abdollahi A, Fathi M (2020) An intrusion detection system on ping of death attacks in IoT networks. *Wireless Personal Communications*, 112: 2057–2070, doi:10.1007/s11277-020-07139-y.
- [42] Khan Y, Su'ud MBM, Alam MM, Ahmad SF, Salim NA, Khan N (2023) Architectural threats to security and privacy: A challenge for internet of things (IoT) applications. *Electronics*, 12: 88, doi:10.3390/electronics12010088.
- [43] Forsström S, Butun I, Eldefrawy M, Jennehag U, Gidlund M (2018) Challenges of securing the industrial internet of things value chain. In: *2018 Workshop on Metrology for Industry 4.0 and IoT*, 218–223. IEEE, Brescia.
- [44] Ghorbani AA, Lu W, Tavallaee M (2009) Network intrusion detection and prevention: concepts and techniques. In: *Advances in Information Security*. Springer, New York, vol. 47.
- [45] Spathoulas GP, Katsikas SK (2010) Reducing false positives in intrusion detection systems. *Computers & Security*, 29(1): 35–44.
- [46] Concha A, et al. (2014) Using sniffing behavior to differentiate true negative from false negative responses in trained scent-detection dogs. *Chemical Senses*, 39(9): 749–754.
- [47] Gautam KS, Om H (2016) Computational neural network regression model for host based intrusion detection system. *Perspectives on Science*, 8: 93–95.
- [48] Macia-Perez F, Mora-Gimeno FJ, Marcos-Jorquera D, Gil-Martinez-Abarca JA, Ramos-Morillo H, Lorenzo-Fonseca I (2011) Network intrusion detection system embedded on a smart sensor. *IEEE Transactions on Industrial Electronics*, 58(3): 722–732.
- [49] Hong J, Liu C, Govindarasu M (2014) Integrated anomaly detection for cyber security of the substations. *IEEE Transactions on Smart Grid*, 5(4): 1643–1653.
- [50] Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys and Tutorials*, 16(1): 303–336.
- [51] Mishra P, Pilli ES, Varadharajan V, Tupakula U (2017) Intrusion detection techniques in cloud environment: A survey. *Journal of Network and Computer Applications*, 77: 18–47.
- [52] Duque S, bin Omar MN (2015) Using data mining algorithms for developing a model for intrusion detection system (IDS). *Procedia Computer Science*, 61: 46–51.
- [53] Amin SO, Siddiqui MS, Hong CS, Lee S (2009) RIDES: Robust intrusion detection system for IP-based ubiquitous sensor networks. *Sensors*, 9(5): 3447.

- [54] Bul'ajoul W, James A, Pannu M (2015) Improving network intrusion detection system performance through quality of service configuration and parallel technology. *Journal of Computer and System Sciences*, 81(6): 981–999.
- [55] Hubballi N, Suryanarayanan V (2014) False alarm minimization techniques in signature-based intrusion detection systems: A survey. *Computer Communications*, 49: 1–17, ISSN 0140–3664, doi:10.1016/j.comcom.2014.04.012.
- [56] Kruegel C, Toth T (2003) “Using decision trees to improve signature-based intrusion detection,” In *International workshop on recent advances in intrusion detection*, Springer Berlin Heidelberg, Germany, pp. 173–191.
- [57] Veeramreddy J, Prasad V, Prasad K (2011) A review of anomaly based intrusion detection systems. *International Journal of Computer Applications*, 28: 26–35, doi:10.5120/3399–4730.
- [58] Chauhan P, Chandra N (2013) A review on hybrid intrusion detection system using artificial immune system approaches. *International Journal of Computer Applications*, 68: 22–27, doi:10.5120/11695–6499.
- [59] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J, Alazab A (2019) A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. *Electronics*, 8(11): 1210, doi:10.3390/electronics8111210.
- [60] Maleh Y, Ezzati A, Qasmaoui Y, Mbida M (2015) A global hybrid intrusion detection system for wireless sensor networks. *Procedia Computer Science*, 52: 1047–1052, ISSN 1877-0509, doi:10.1016/j.procs.2015.05.108.
- [61] Tsai JJP, Yu PS, eds. (2009) *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*, 1st edn. Springer-Verlag, Springer Science & Business Media, New York, pp. 1–362.
- [62] Nishani L, Biba M (2016) Machine learning for intrusion detection in MANET: A state-of-the-art survey. *Journal of Intelligent Information Systems*, 46(2): 391–407.
- [63] Namdev N, Agrawal S, Silkari S (2015) Recent advancement in machine learning based internet traffic classification. *Procedia Computer Science*, 60: 784–791.
- [64] Olufowobi H, Young C, Zambreno J, Bloom G (2019) Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing. *IEEE Transactions on Vehicular Technology*, 69: 1484–1494.
- [65] Eskandari M, Janjua ZH, Vecchio M, Antonelli F (2020) Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*, 7: 6882–6897, doi:10.1109/JIOT.2020.2970501.
- [66] Kumar V, Das AK, Sinha D (2020) Statistical analysis of the UNSW-NB15 dataset for intrusion detection. In: *Computational Intelligence in Pattern Recognition*. Springer, Singapore, pp. 279–294.
- [67] Mehmood A, Khanan A, Umar MM, Abdullah S, Ariffin KAZ, Song H (2017) Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access*, 6: 5688–5694.
- [68] Sabeel U, Chandra N (2013) Categorized security threats in the wireless sensor networks: Countermeasure and security management schemes. *International Journal of Computer Applications*, 64: 19–28.
- [69] Hummen R, Hiller J, Wirtz H, Henze M, Shafagh H, Wehrle K (2013) 6LoWPAN fragmentation attacks and mitigation mechanisms. In: *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*. ACM, Darmstadt Germany, pp. 55–66.
- [70] Kasinathan P, Pastrone C, Spirito MA, Vinkovits M (2013) Denial-of-service detection in 6LoWPAN based internet of things. In: *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, Lyon, France, pp. 600–607.

- [71] Kasinathan P, Costamagna G, Khaleel H, Pastrone C, Spirito MA (2013) An IDS framework for internet of things empowered by 6LoWPAN. In: *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. ACM, Berlin Germany, pp. 1337–1340.
- [72] Scarfone K, Mell P (2007) Guide to intrusion detection and prevention systems (IDPS). *NIST Special Publication*, 800: 94.
- [73] Yar H, Hussain T, Khan ZA, Koundal D, Lee MY, Baik SW (2021) Vision sensor-based real-time fire detection in resource-constrained IoT environments. *Computational Intelligence and Neuroscience*, 2021: 15, Article ID 5195508.
- [74] Islam N, Altamimi M, Haseeb K, Siraj M (2021) Secure and sustainable predictive framework for IoT-based multimedia services using machine learning. *Sustainability*, 13(23), Article ID 13128.
- [75] Wu Y, Wei D, Feng J (2020) Network attacks detection methods based on deep learning techniques: A survey. *Security and Communication Networks*, 2020: 17, Article ID 8872923, doi:10.1155/2020/8872923.
- [76] Tang TA, Mhamdi L, McLernon D, Zaidi SAR, Ghogho M (Oct. 2016) Deep learning approach for network intrusion detection in software defined networking. In: *Proceedings of 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM)*. IEEE, Reims, France, pp. 258–263.
- [77] Kolosnjaji B, Zarras A, Webster G, Eckert C (Dec. 2016) Deep learning for classification of malware system call sequences. In: *Proceedings of Australasian Joint Conference on Artificial Intelligence*. Springer, Hobart, Australia, pp. 137–149.
- [78] Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access*, 5: 21954–21961.
- [79] Gao N, Gao L, Gao Q, Wang H (Nov. 2014) An intrusion detection model based on deep belief networks. In: *Proceedings of 2014 Second International Conference on Advanced Cloud and Big Data*. IEEE, Huangshan, China, pp. 247–252.
- [80] Erpek T, Sagduyu YE, Shi Y (2018) Deep learning for launching and mitigating wireless jamming attacks. *IEEE Transactions on Cognitive Communications and Networking*, 5(1): 2–14.
- [81] Yu Y, Long J, Cai Z (2017) Network intrusion detection through stacking dilated convolutional autoencoders. *Security and Communication Networks*, 2017: 10, Article ID 4184196.
- [82] Li Y, Ma R, Jiao R (2015) A hybrid malicious code detection method based on deep learning. *International Journal of Security and Its Applications*, 9(5): 205–216.
- [83] Sourour M, Adel B, Tarek A (2011) Network security alerts management architecture for signature-based intrusions detection systems within a NAT environment. *Journal of Network and Systems Management*, 19(4): 472–495.
- [84] Zhang Y, et al. (2011) Distributed intrusion detection system in a multi-layer network architecture of smart grids. *IEEE Transactions on Smart Grid*, 2(4): 796–808.
- [85] Atefinia R, Ahmadi M. (2021) Network intrusion detection using multi-architectural modular deep neural network. *The Journal of Supercomputing*, 77: 3571–3593.
- [86] Sangeetha S, et al. (2015) Signature based semantic intrusion detection system on cloud. In: *Information Systems Design and Intelligent Applications: Proceedings of Second International Conference INDIA 2015*. Springer, Kalyani, India, vol. 1.
- [87] Hamdi O, Mbaye M, Krief F (2015) A cloud-based architecture for network attack signature learning. In: *2015 7th International Conference on New Technologies, Mobility and Security (nTMS)*. IEEE, Paris, France.
- [88] Otoum Y, Nayak A (2021) As-ids: Anomaly and signature based ids for the internet of things. *Journal of Network and Systems Management*, 29: 1–26.
- [89] Jyothsna, VVRPV, Prasad R, Prasad KM (2011) A review of anomaly-based intrusion detection systems. *International Journal of Computer Applications*, 28(7): 26–35.

- [90] Khan S, Motwani D (2017) Implementation of IDS for web application attack using evolutionary algorithm. In: *2017 International Conference on Intelligent Computing and Control (I2C2)*. IEEE, Coimbatore, India.
- [91] Meng W, Li W, Kwok L-F (2014) EFM: Enhancing the performance of signature-based network intrusion detection systems using enhanced filter mechanism. *Computers & Security*, 43: 189–204.
- [92] Uddin M, Rahman AA (2010) Dynamic multilayer signature-based intrusion detection system using mobile agents. *arXiv preprint arXiv:1010.5036*.
- [93] Bronte R, Shahrir H, Haddad HM (2016) A signature-based intrusion detection system for web applications based on genetic algorithm. In: *Proceedings of the 9th International Conference on Security of Information and Networks*. ACM, Newark NJ USA.
- [94] Khan I, Hassan M, Aziz M (2021) Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS. *Computers, Materials and Continua*, 70: 3654–3665, doi:10.32604/cmc.2022.020697.
- [95] Khan IU, Hassan MA, Alshehri MD, Ikram MA, Alyamani HJ, Alturki R, Hoang VT (2021) Monitoring system-based flying IoT in public health and sports using ant-enabled energy-aware routing. *Journal of Healthcare Engineering*, 2021: 11, Article ID 1686946, doi:10.1155/2021/1686946.
- [96] Shah SN, Singh MP. (2012) Signature-based network intrusion detection system using SNORT and WINPCAP. *International Journal of Engineering Research & Technology (IJERT)*, 1(10): 1–7.
- [97] Khan IU, Abdollahi A, Alturki R, Alshehri MD, Ikram MA, Alyamani HJ, Khan S (2021) Intelligent detection system enabled attack probability using Markov chain in aerial networks. *Wireless Communications and Mobile Computing*, 2021: 9, Article ID 1542657, doi:10.1155/2021/1542657.

9 Hybrid Model for IoT-Enabled Intelligent Towns Using the MQTT-IoT-IDS2020 Dataset

Zupash, Muhammad Allah Rakha, Inam Ullah Khan, Mariya Ouaisa, Mariyam Ouaisa, and Muhammad Yaseen Ayub

9.1 INTRODUCTION

Population growth drives urbanization, stressing all aspects of city life. Cities are known for their dense concentrations of amenities and resources, which attract residents from remote regions. As a result, the need for effective city management has become a top priority for city politics and administration. IoT-enabled smart cities are considered a long-term solution for these problems. Many companies have invested in the IT industry to automate the entire processes of smart cities. Public and private sectors are interested in providing optimal solutions. Wireless connected IoT devices are quite popular in the concept of smart cities. IoT applications are utilized in many fields of study, including smart homes, healthcare, transportation, parking, education, public safety, and monitoring. IoT devices continuously connect with people and things in smart cities [1, 2]. Moreover, IoT is primarily driven by technological advancements that facilitate humans. The idea of intelligent towns has emerged from advanced IoT, which offers a new avenue for sustainable development. Intelligent communication, processing, and physical infrastructure are important factors for IoT networks. IoT architecture faces many security, data privacy, and end-to-end delay issues that directly affect the entire network [3].

Smart city networks are connected through IoT devices, which face several challenges due to the huge amount of data. However, security applications and tools will be quite helpful for detecting third party, malware, DoS, DDoS, DNS, and ping of death attacks. Still, there exist many challenges that need to be addressed, such as cyber terrorism, third-party mirroring, cyber crime, and high latency. Smart policy is an essential tool to establish liaison between users and research centers, while to provide a knowledge-based intelligent framework to support smart defense policy. Cyber attacks usually damage all network operations. Cyber attacks must be monitored to identify abnormal data packets. Moreover, the rise of IoT devices in every

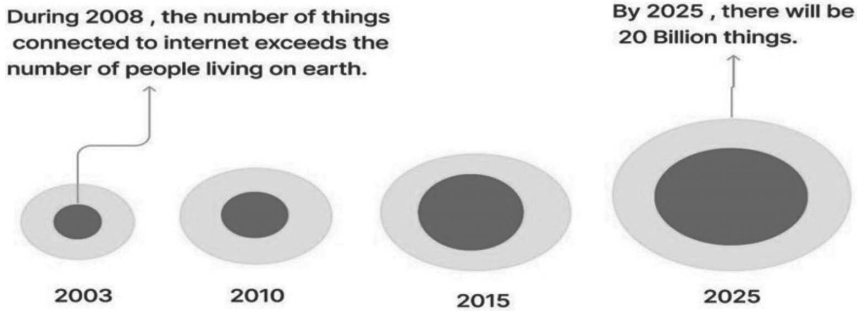


FIGURE 9.1 Growth of IoT-connected devices.

industry is in demand. Therefore, new applications for IoT networks in smart cities will detect cyber attacks [4]. Figure 9.1 presents significant growth in IoT devices, where there will be around 20 billion IoT devices in the smart world by 2025.

Due to cyber attacks, IoT networks are quite vulnerable. Network intrusion detection systems identify spoof-based data packets. Intrusion detection systems monitor network traffic through which fake data packets can be detected easily. However, security information and event management (SIEM) systems record unknown behavior, violation, and information sent to the system administrator. SIEM systems directly filter false alarm data packets from IoT networks. In addition, hybrid intrusion detection systems (HIDS) are considered the optimal solution to detect possible cyber attacks using machine learning. Intruders reduce false positive rates, and misdetection increases. Although optimal decisions can be made possible using machine-learning-enabled IDS, machine learning techniques are used to test and train datasets. IDSs use a range of machine learning techniques to find cyber attacks on systems in intelligent towns. A chosen machine learning method or a collection of ML methods trains and tests the data to differentiate between harmful and normal nodes. The effectiveness of identifying malicious nodes depends on the deployment location of IDS and dependable datasets of security threats for the training process [5–7].

9.2 LITERATURE STUDY

This section is related to the limitations of intrusion detection systems (IDS) in IoT networks. These networks have fewer resources, so intruders deploy various attacks such as ping of death (PoD), denial of service (DoS), and distributed denial of service (DDoS) to limit overall resources. Intruders continuously send fake data packets to degrade the entire IoT network. However, anomaly-based IDS filters data packets. Moreover, false alarms, high accuracy, and queue length are considered the main problems in IDS [8]. Furthermore, IoT easily connects users, information, and devices through wireless communication technologies. Cyber attacks are considered a direct threat to IoT networks. A Markov-chain-enabled IDS is formulated to detect possible cyber attacks. A novel threshold has been designed that balances

false positive and false negative using the Markov chain distribution. Queue length, packet loss, high detection rate, and accuracy are major problems in IoT-enabled IDS [9]. Accordingly, many researchers around the world are using machine-learning-based techniques to provide better solutions. Intelligent communication systems are basically the need of the day. Ullah et al. discussed techniques related to intelligent transportation systems, cyber security, UAVs, 5G communication, and healthcare in the field of smart cities. An agent-based learning mechanism is discussed in terms of smart cities to improve the quality of service [10]. Energy is the main problem in IoT-enabled UAVs. Therefore, the E-AntHocNet routing protocol is designed to improve the energy level in the UAV network [11]. In addition, artificial intelligence and machine learning approaches are quite useful in smart cities. Machine learning techniques are helpful in the real-time analysis of town activities. IoT networks can be easily deployed in smart cities where network congestion in data traffic is the main problem. Due to that, an adaptive technique is utilized to lower the number of data packets, which will reduce congestion [12]. IDS has three main subcategories: anomaly, signature, and hybrid. H-IDS recognizes misuse detection, reduces false alarms, and maintains high accuracy. A fuzzy inference-based hybrid IDS has been designed that identifies cyber attacks [13].

9.3 IOT DESIGN AND ARCHITECTURE

Many companies are investing in IoT devices. However, the Internet is the backbone used in IoT networks. Moreover, the integration of people, objects, and things is the combination of IoT. The IoT framework aims to connect the real and virtual worlds with one another. Machine-to-machine communication is the main foundation of IoT. Although IoT equipment is widely utilized, the concept of smart cities mainly relies on IoT networks. Accordingly, smart homes offer IoT-enabled connectivity for power management and automation. However, the concept of intelligent towns is becoming more of a reality with IoT systems [14–16].

IoT uses a special kind of architecture that includes application, network, and perception layers. Almost every layer needs security to ensure communication. Figure 9.2 presents a three-layered IoT design and architecture. The network layer is responsible for data transmission between IoT nodes. The perception layer uses physical mainly IoT devices to collect information [17].

Figure 9.3 describes a five-layered IoT architecture that has some distinct functions. The perception and application layers perform the same tasks as in the previous model. Data processing can be made possible in the network layer. However, the network layer easily transfers data packets from sender to receiver using wireless communication technologies, which include 3G, 4G, LTE, 5G, Wi-Fi, and Bluetooth. In addition, the business layer easily visualizes overall data that satisfies future goals. Further research is needed to improve the entire IoT-enabled architecture [18].

IoT-based sensors play an important role while collecting information. IoT devices are utilized in many different applications. While the actuator easily moves the IoT workstation, this technology has applications in healthcare, transportation, rescue operations, and many other areas [19–21]

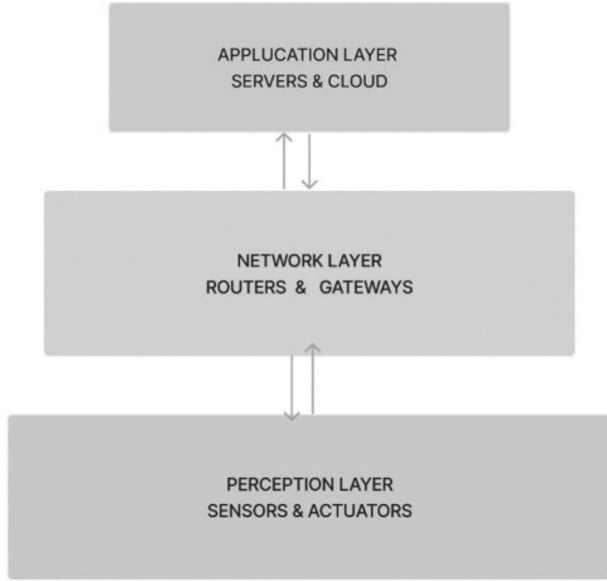


FIGURE 9.2 Three-layered IoT Design and architecture.

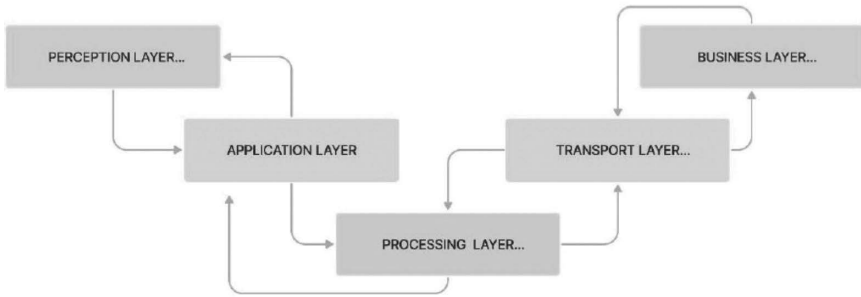


FIGURE 9.3 Five-layered IoT architecture.

9.4 INTEGRATION OF IOT IN INTELLIGENT TOWNS

The merger of IoT with intelligent towns is considered a novel concept in research and development. Over the past few years, IoT-enabled sensors have been improved, and IoT has become the primary technology used in smart towns. Interestingly, intelligent towns have emerged from the concept of modern smart cities, as many problems such as unemployment, health, and education have been observed in smart cities. Therefore, intelligent towns are expected to address these problems using information communication technologies. They feature modern ways of living, governance, transportation, and business, all of which can be improved with IoT. An IoT-enabled intelligent town can significantly improve the living standards of

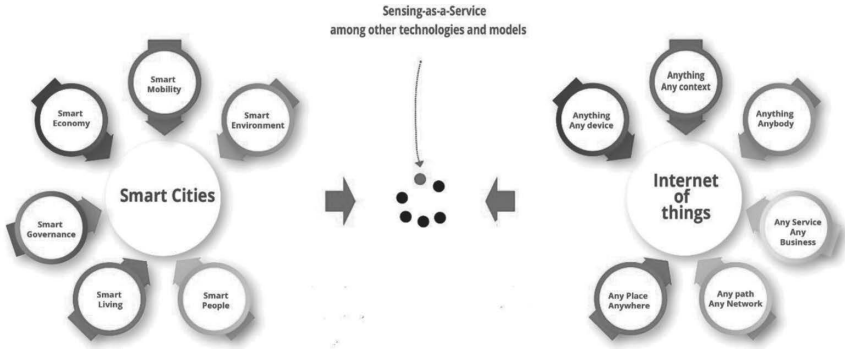


FIGURE 9.4 Relationship between IoT and intelligent towns.

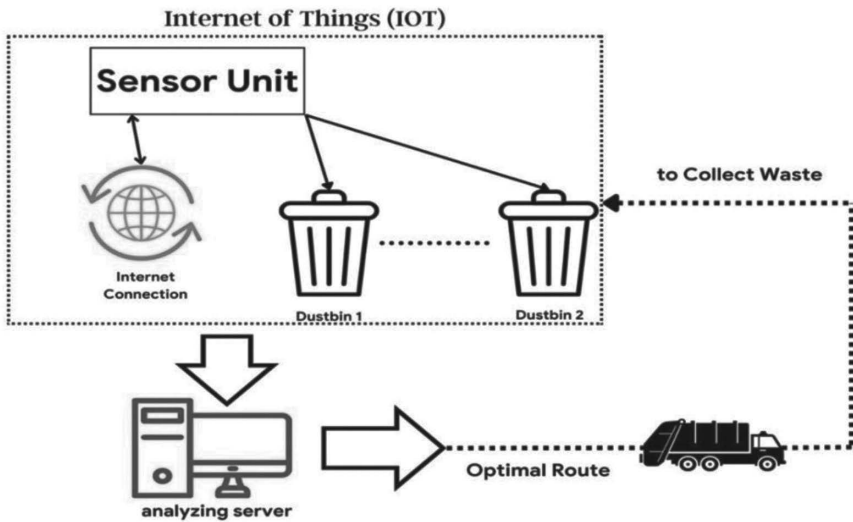


FIGURE 9.5 IoT-enabled waste collection.

its residents. Figure 9.4 presents an idea of smart cities and the Internet of Things. Machine learning classifiers play an essential role in decision making by collecting information from IoT sensor nodes. Wireless-enabled intelligent towns have reduced end-to-end delay [22–25].

Figure 9.5 illustrates the process of waste collection enabled by IoT. According to this novel IoT technology, the waste collection process is improved. However, machine learning techniques can provide innovative solutions in near future.

9.5 CYBER ATTACKS IN INTELLIGENT TOWNS

Integration of IoT with intelligent towns has improved the overall quality of experience. Also, due to wireless technologies, intelligent towns are extremely vulnerable

to cyber attacks, do a decision support system is quite relevant. Therefore, the cyber security risk needs to be reduced. Moreover, denial of service, distributed denial of service, and ping of death attacks are quite dangerous and capable of hijacking an entire network [26–28].

9.6 INTRUSION DETECTION SYSTEM FOR IOT NETWORK

Information sharing is increased due to social media platforms; therefore, security need to be ensured. Cyber threats are usually launched to gain access of entire IoT network. Therefore, intrusion detection is designed to identify possible cyber attacks. There are around four major types of IDS: network-IDS, hybrid-IDS, anomaly-IDS, and signature-IDS. Also, data privacy is considered a major problem in smart cities. IDS is used to monitor and ensure reliable IoT operations. False alarms, accuracy, precision, recall, and F1-score can all be improved using machine learning and deep learning classifiers [29–32].

9.7 ANOMALY-BASED IDS

Anomaly-based intrusion detection systems are used to have novel threshold in order to detect possible cyber attacks. Figure 9.6 presents various anomaly-based IDS techniques. Anomaly-IDS is considered an updated model to identify abnormal data packets. These days, machine-learning-enabled anomaly-based IDS are widely utilized by many researchers and engineers [33–38].

9.8 HYBRID-BASED IDS

In today’s era, the hybrid-based IDS is the best possible practice to secure an IoT network. Hybrid-IDS is basically the combination of signature and anomaly. Large

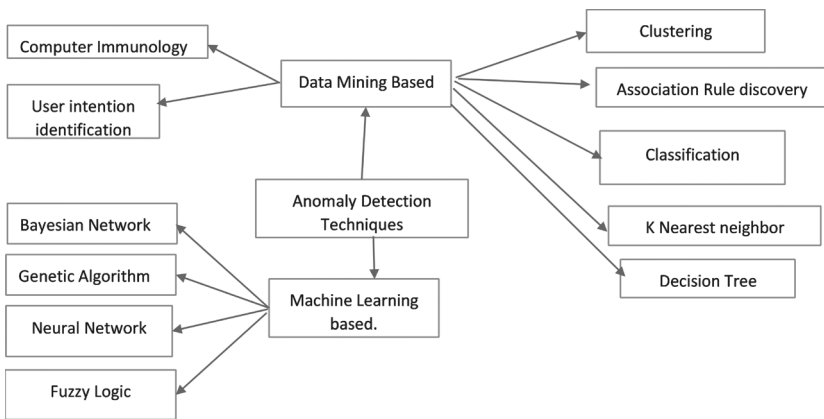


FIGURE 9.6 Methods of intrusion based on anomalies.

amounts of data can be easily monitored using hybrid-IDS. However, hybrid-IDSs easily detect suspicious intrusions from unknown nodes. Recently, many researchers are using machine learning and deep learning for hybrid IDS to secure communication channels [39–41].

9.9 MQTT-IOT-IDS2020 DATASET

Datasets are used to represent some specific data. Therefore, general purpose datasets are utilized to check overall performance. MQTT-IoT-IDS2020 is used in a simulation environment. MQTT is quite helpful for machine-to-machine communication. During experimentation uniflow and biflow metrics are utilized to calculate accuracies [42–45].

9.10 PROPOSED HYBRID MODEL

The hybrid model is the combination of ConvID and the long short-term memory network (LSTM) approach.

The model includes an input layer that consists of both input and output. Additionally, Figure 9.7 provides an overview of the entire process of the hybrid model.

9.11 SIMULATION RESULTS

MQTT-IDS2020 is having new data where uniflow, biflow, precision, recall, F1-score, and accuracies are used to check performance. Around six traditional classifiers, which include logistic regression, *K*-NN, Gaussian naïve Bayes, decision tree, Adaboost, and random forest, are compared with the proposed hybrid model. Also, during experimentation, binary classification is used.

9.11.1 UNIFLOW

Figure 9.8 shows ROC curve data analysis where the true positive and false positive rates are used for evaluation. However, the hybrid model shows better results in comparison with other traditional techniques.

In Figure 9.9, three important parameters, namely precision, recall, and F1-score, are presented. The results of the hybrid model, logistic regression, decision tree, Adaboost, and random forest show optimal results, while the GaussianNB classifier displays poor results in comparison to the other models.

Figure 9.10 illustrates two different scenarios: attack and no attack. During uniflow experimentation, 75.9 % had no attack, and 24.1% had attack.

Figure 9.11 illustrates the accuracies of different techniques, and it can be observed that the hybrid model has an accuracy of approximately 99.77599.

Figure 9.12 presents a comparison of precision scores for various techniques used for intrusion detection in IoT. The results show that the hybrid model has the highest precision score, while the GaussianNB technique performance is very low as compared to other methods.

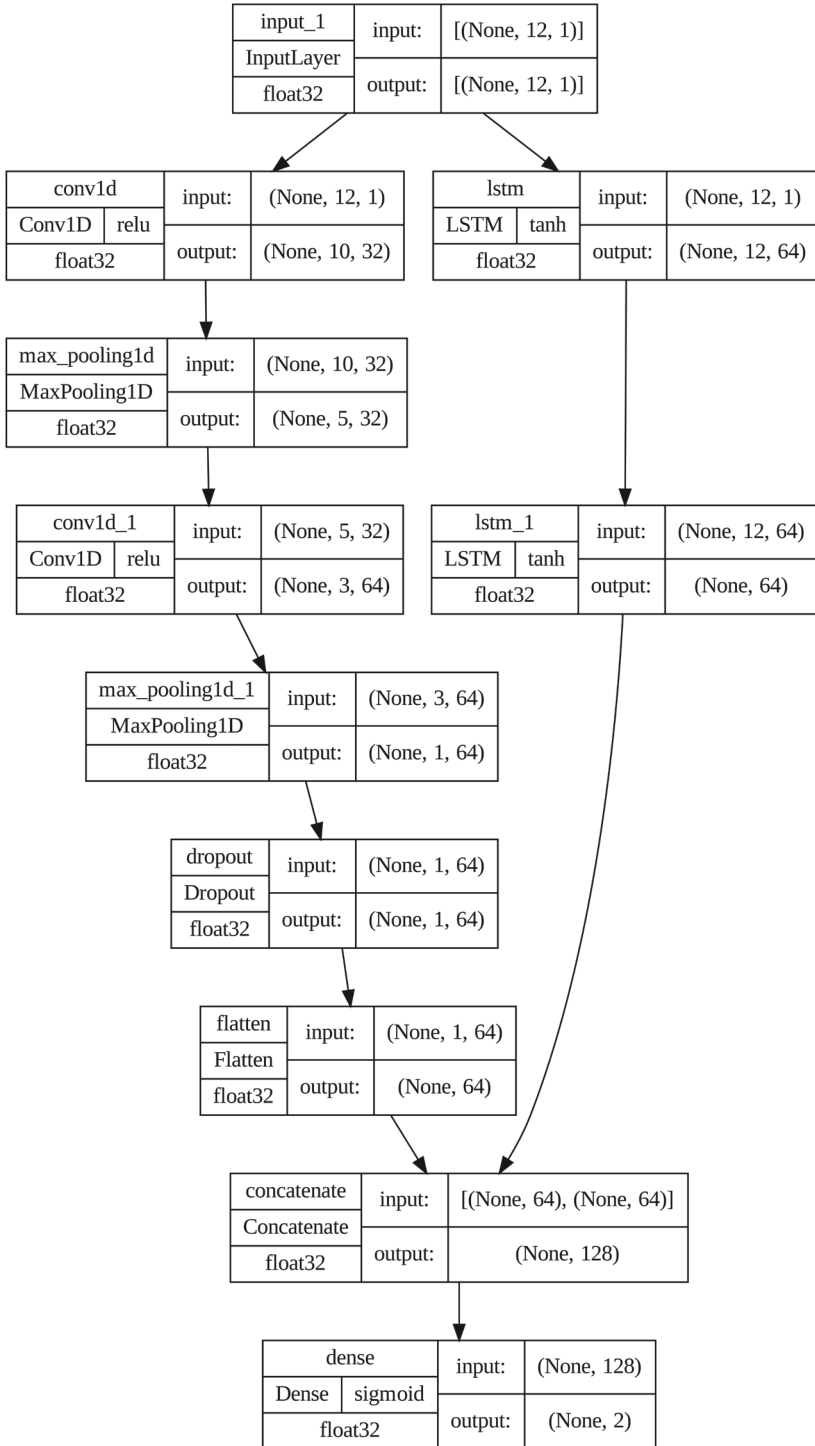


FIGURE 9.7 Proposed hybrid model.

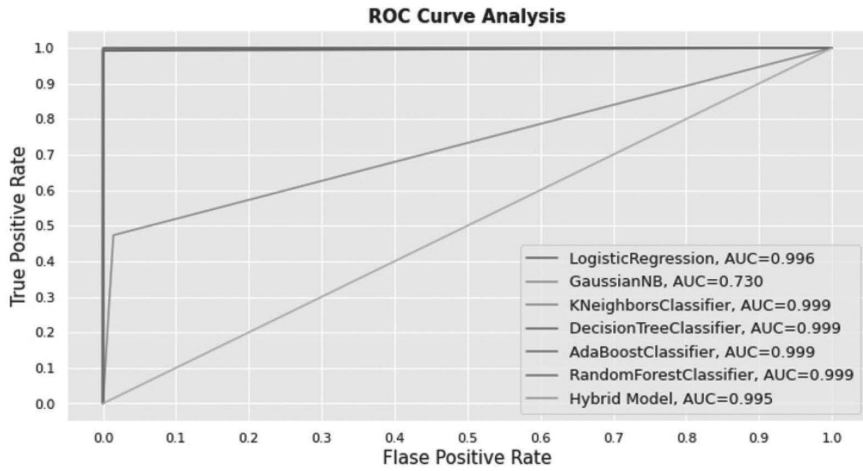


FIGURE 9.8 ROC curve analysis.

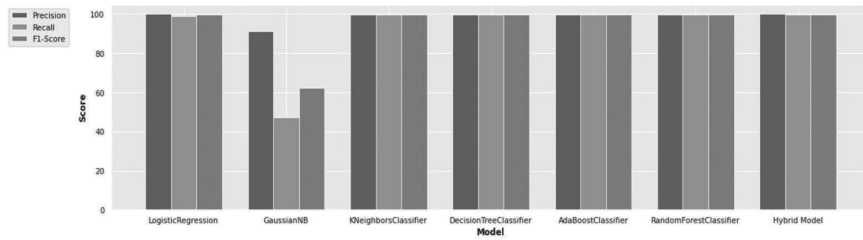


FIGURE 9.9 Precision, recall, and F1-score using uniflow.

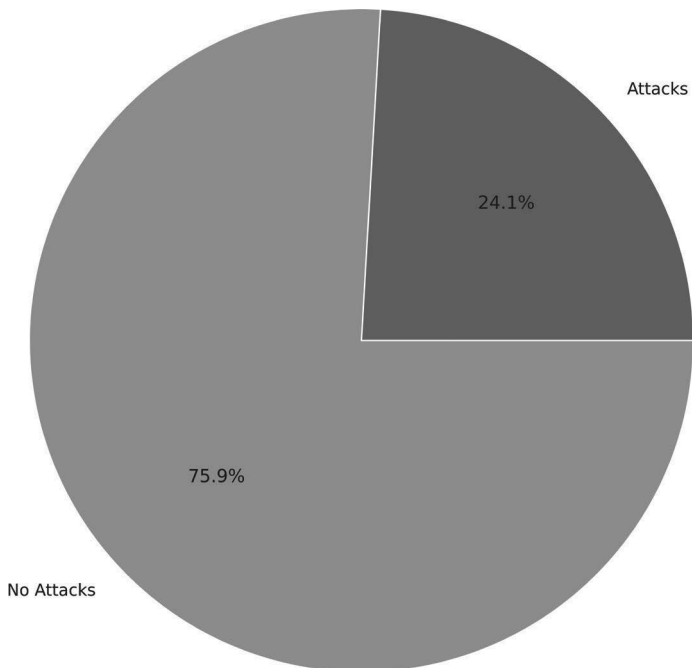


FIGURE 9.10 Percentage of data with attack and without attack.

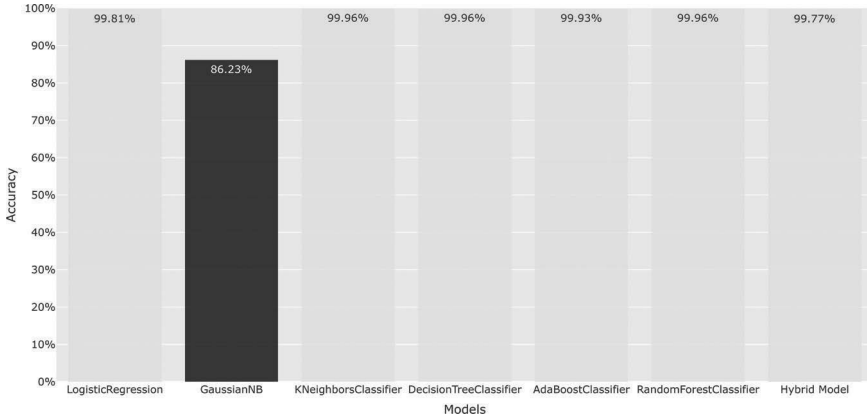


FIGURE 9.11 Accuracies of logistic regression, K -NN, Gaussian naïve Bayes, decision tree, Adaboost, random forest, and hybrid model

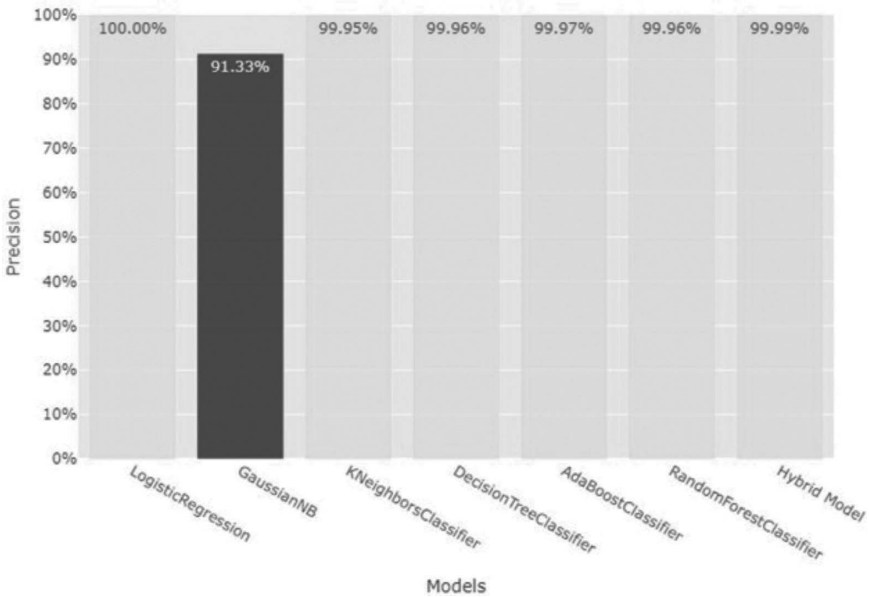


FIGURE 9.12 Precision results of logistic regression, K -NN, Gaussian naïve bayes, decision tree, Adaboost, random forest, and hybrid model.

Figure 9.13 presents results regarding F1-score.

Figure 9.14 illustrates the recall metric where hybrid model scores around 99.74%.

Table 9.1 summarizes the data presented in Figures 9.11, 9.12, 9.13, and 9.14.

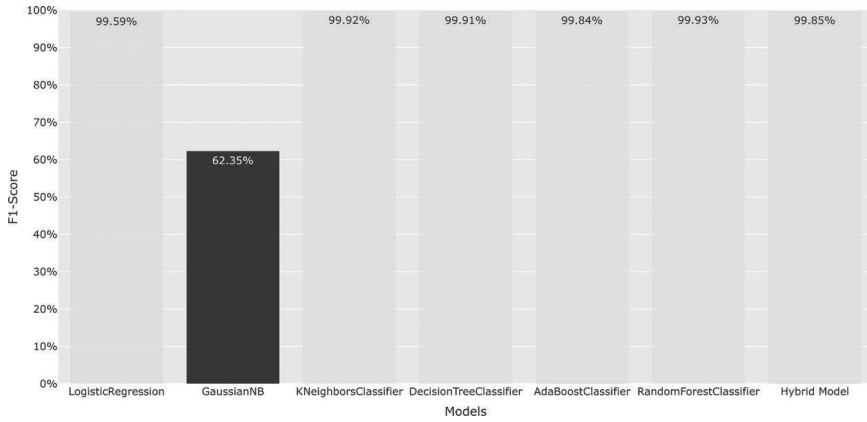


FIGURE 9.13 F1-score using uniflow.

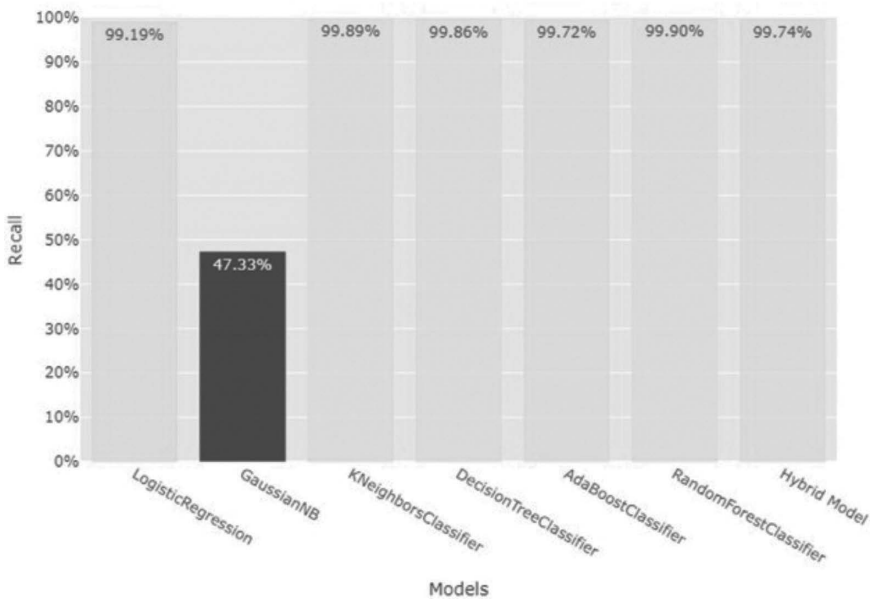


FIGURE 9.14 Recall metric using uniflow.

TABLE 9.1
Metrics Include Accuracy, Precision, Recall, and F1-Score for Uniflow

Models	Accuracy	Precision Score	Recall Score	F1-Score
Logistic regression	99.80526	100	99.19139	99.59405
GaussianNB	86.23177	91.32509	47.32696	62.34512
K-NN classifier	99.96166	99.95388	99.88688	99.92037
Decision tree classifier	99.95661	99.96225	99.85755	99.90987
AdaBoost classifier	99.92533	99.9706	99.71929	99.84479
Random forest classifier	99.96468	99.95808	99.89526	99.92666
Hybrid model (proposed)	99.77599	99.98937	99.71634	99.85267

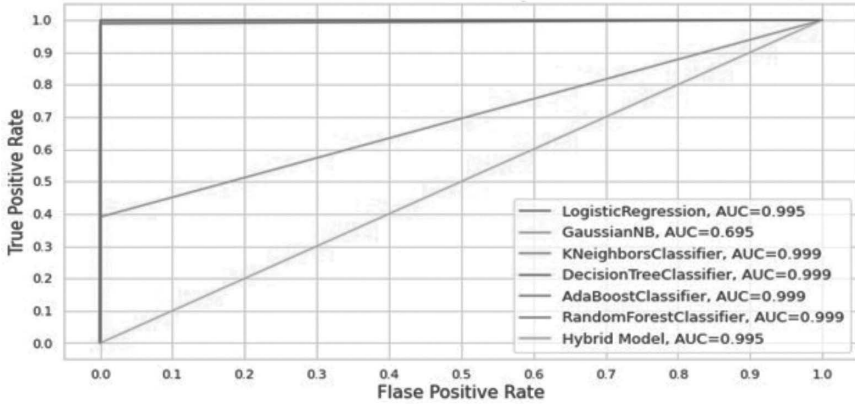


FIGURE 9.15 ROC curve analysis using biflow.

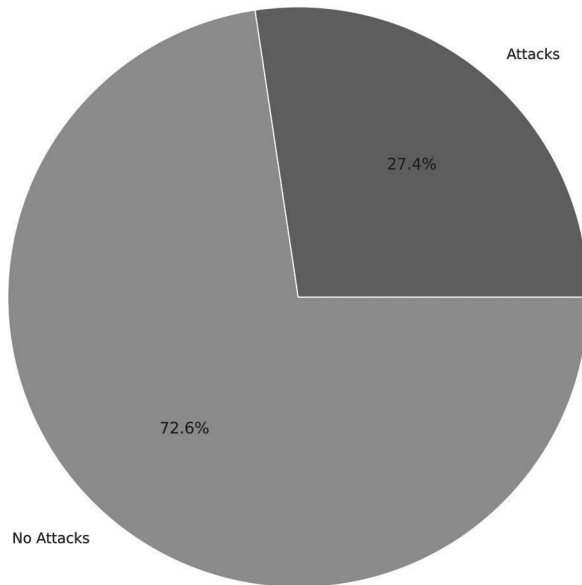


FIGURE 9.16 Percentages of data representing attack and no attack using biflow.

9.11.2 BIFLOW SIMULATION RESULTS

Various figures present simulation results regarding biflow where accuracy, precision, recall, F1-score, and two different scenarios are discussed in detail. Figure 9.15 shows simulation results related to the true positive and false positive rates. Six different classifiers were utilized for comparison with the hybrid model.

In Figure 9.16, the detection results of attacks and no attacks are presented. Specifically, it can be observed that 27.4% of the monitored areas are reported to have attacks, while 72.6% do not.

Figure 9.17 presents information regarding the accuracies of various models. The proposed hybrid model, along with *K*-NN, decision tree, AdaBoost, and random forest show better results.

Figure 9.18 illustrates simulation results related to precision. More interestingly, the hybrid model and logistic regression performance results are outstanding.

Figure 9.19 presents information on the F1-score metric. *K*-NN, Adaboost, and the proposed hybrid model are shown to have outstanding results in comparison to the other models.

Figure 9.20 depicts information related to recall. GaussianNB has very low results of around 39.08% in comparison with the other techniques.

Additionally, the data presented in Figures 9.17, 9.18, 9.19, and 9.20 is summarized in Table 9.2.

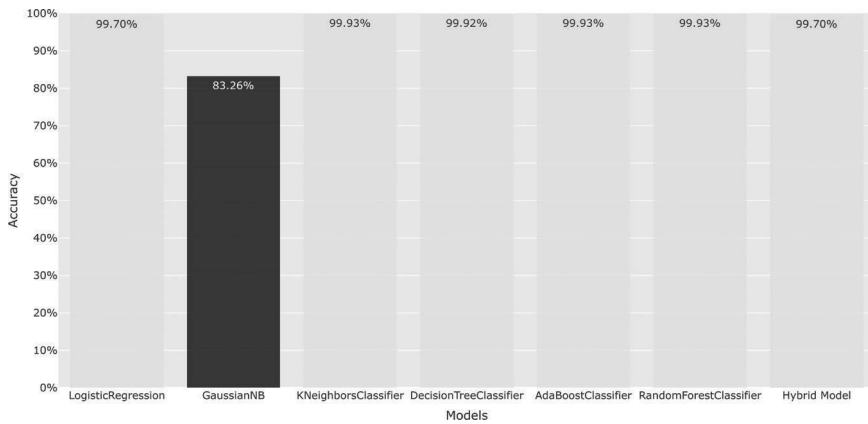


FIGURE 9.17 Accuracies of various models using biflow.

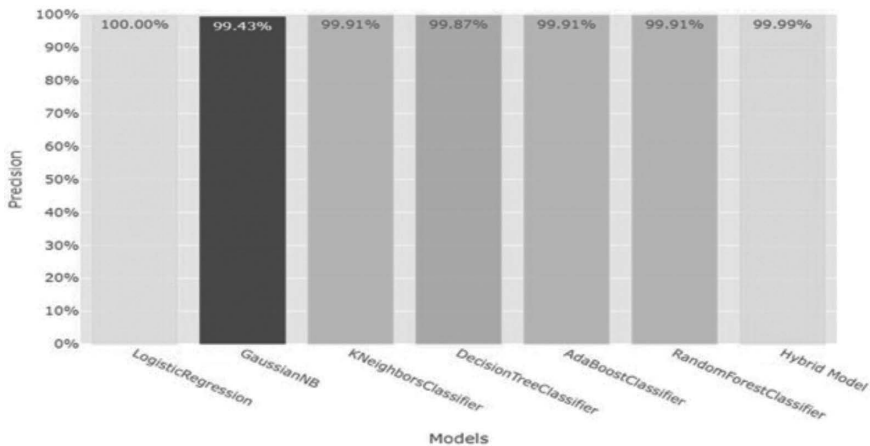


FIGURE 9.18 Simulation result of precision using biflow.

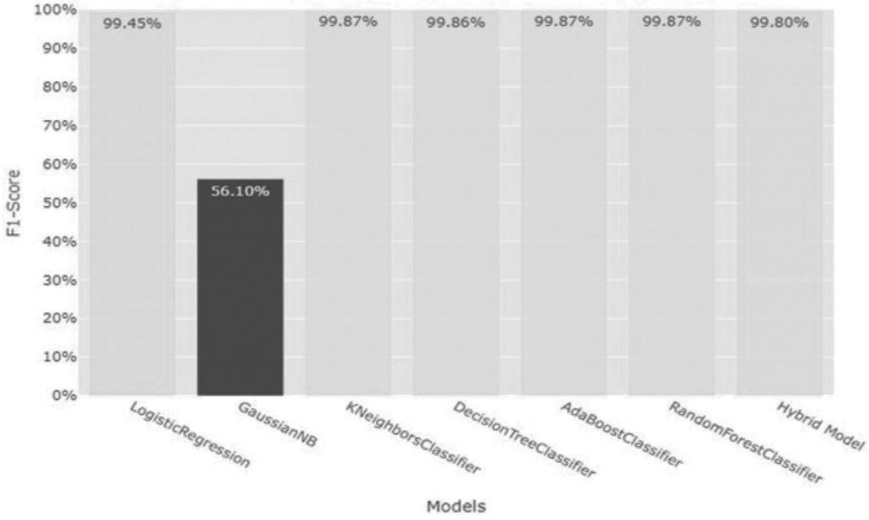


FIGURE 9.19 F1-score simulation result using biflow.

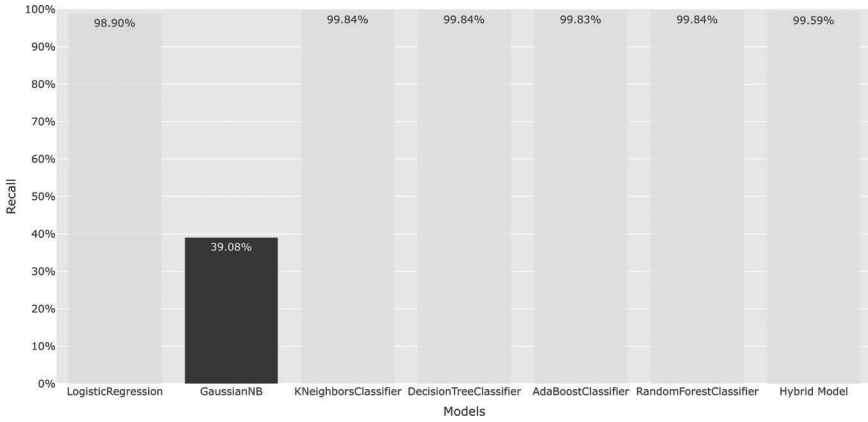


FIGURE 9.20 Recall simulation metric for biflow.

TABLE 9.2
Models with Different Metrics Numerical Results

Models	Accuracy	Precision Score	Recall Score	F1-Score
Logistic regression	99.69928	100	98.90141	99.44767
GaussianNB	83.26201	99.42663	39.07746	56.10434
K-NN-classifier	99.9306	99.90839	99.83803	99.87319
Decision tree classifier	99.92097	99.87319	99.83803	99.85561
AdaBoost classifier	99.92868	99.90838	99.83099	99.86967
Random forest classifier	99.9306	99.90839	99.83803	99.87319
Hybrid model (proposed technique)	99.70892	99.98673	99.61393	99.79998

9.12 CONCLUSIONS AND FUTURE DIRECTIONS

IoT with intelligent towns improve overall communication. MQTT-IoT-IDS2020 is used for simulation to evaluate various models. The proposed hybrid approach performed better in contrast with other models. Six traditional techniques are utilized to compare simulation results with the hybrid model. Machine learning and deep learning models can be applied in many different fields of study. Binary classification is performed in a simulation environment. Precision, recall, F1-score, and accuracies metrics are used for unifiow and biflow. IoT design and architecture, cyber attacks on IoT networks, and intrusion detection system were briefly discussed. Also, the novel concept of IoT with intelligent towns is well explained. In near future, machine learning, deep learning, neural networks, and heuristic computations will heighten accuracies and reduce false alarms.

REFERENCES

1. Perera, C., Zaslavsky, A., Christen, P. and Georgakopoulos, D., 2014. Sensing as a service model for smart cities supported by internet of things. *Transactions on Emerging Telecommunications Technologies*, 25(1), pp. 81–93.
2. Almiyani, M., AbuGhazleh, A., Al-Rahayfeh, A., Atiewi, S. and Razaque, A., 2020. Deep recurrent neural network for IoT intrusion detection system. *Simulation Modelling Practice and Theory*, 101, p. 102031.
3. Li, D., Deng, L., Lee, M. and Wang, H., 2019. IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning. *International Journal of Information Management*, 49, pp. 533–545.
4. Edelenbos, J., Hirzalla, F., van Zoonen, L., van Dalen, J., Bouma, G., Slob, A. and Woestenburg, A., 2018. Governing the complexity of smart data cities: Setting a research agenda. *Smart Technologies for Smart Governments: Transparency, Efficiency and Organizational Issues*, pp. 35–54.
5. Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. and Alazab, A., 2020. Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics*, 9(1), p. 173.
6. Farias, R.S., de Souza, R.M., McGregor, J.D. and de Almeida, E.S., 2019. Designing smart city mobile applications: An initial grounded theory. *Empirical Software Engineering*, 24, pp. 3255–3289.
7. Mohandas, P., Dhanaraj, J.S.A. and Gao, X.Z., 2019. Artificial neural network based smart and energy efficient street lighting system: A case study for residential area in Hosur. *Sustainable Cities and Society*, 48, p. 101499.
8. Abdollahi, A. and Fathi, M., 2020. An intrusion detection system on ping of death attacks in IoT networks. *Wireless Personal Communications*, 112, pp. 2057–2070.
9. Khan, I.U., Abdollahi, A., Alturki, R., Alshehri, M.D., Ikram, M.A., Alyamani, H.J. and Khan, S., 2021. Intelligent detection system enabled attack probability using Markov chain in aerial networks. *Wireless Communications and Mobile Computing*, 2021, pp. 1–9.
10. Ullah, Z., Al-Turjman, F., Mostarda, L. and Gagliardi, R., 2020. Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, 154, pp. 313–323.
11. Khan, I.U., Qureshi, I.M., Aziz, M.A., Cheema, T.A. and Shah, S.B.H., 2020. Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET). *IEEE Access*, 8, pp. 56371–56378.

12. Ibrahim, A.S., Youssef, K.Y., Eldeeb, A.H., Abouelatta, M. and Kamel, H., 2022. Adaptive aggregation based IoT traffic patterns for optimizing smart city network performance. *Alexandria Engineering Journal*, 61(12), pp. 9553–9568.
13. Tsai, D.R., Tai, W.P. and Chang, C.F., 2003, October. A hybrid intelligent intrusion detection system to recognize novel attacks. In *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings* (pp. 428–434). IEEE.
14. Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M. and Kwak, K.S., 2015. The internet of things for health care: A comprehensive survey. *IEEE Access*, 3, pp. 678–708.
15. Xia, F., Yang, L.T., Wang, L. and Vinel, A., 2012. Internet of things. *International Journal of Communication Systems*, 25(9), p. 1101.
16. Wu, M., Lu, T.J., Ling, F.Y., Sun, J. and Du, H.Y., 2010, August. Research on the architecture of Internet of Things. In *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE)* (Vol. 5, pp. V5–484). IEEE.
17. Tekinerdogan, B., Köksal, Ö. and Çelik, T., 2023. System architecture design of IoT-based smart cities. *Applied Sciences*, 13(7), p. 4173.
18. Zhang, H. and Zhu, L., 2011, June. Internet of things: Key technology, architecture and challenging problems. In *2011 IEEE International Conference on Computer Science and Automation Engineering* (Vol. 4, pp. 507–512). IEEE.
19. Hammoudeh, M. and Arioua, M., 2018. Sensors and actuators in Smart Cities. *Journal of Sensor and Actuator Networks*, 7(1), p. 8.
20. Hu, X., Ji, H. and Liu, L., 2019. Adaptive target birth intensity multi-Bernoulli filter with noise-based threshold. *Sensors*, 19(5), p. 1120.
21. Stojescu-Crisan, C., Crisan, C. and Butunoi, B.P., 2021. An IoT-based smart home automation system. *Sensors*, 21(11), p. 3784.
22. Sundmaeker, H., Guillemin, P., Friess, P. and Woelfflé, S., 2010. Vision and challenges for realising the internet of things. *Cluster of European Research Projects on the Internet of Things, European Commission*, 3(3), pp. 34–36.
23. Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J.R., Mellouli, S., Nahon, K., Pardo, T.A. and Scholl, H.J., 2012, January. Understanding smart cities: An integrative framework. In *2012 45th Hawaii International Conference on System Sciences* (pp. 2289–2297). IEEE.
24. Su, K., Li, J. and Fu, H., 2011. Smart city and the applications. In *2011 International Conference on Electronics, Communications and Control (ICECC)* (pp. 1028–1031). IEEE.
25. Hall, J., Barbeau, M. and Kranakis, E., 2005, August. Anomaly-based intrusion detection using mobility profiles of public transportation users. In *WiMob'2005, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005* (Vol. 2, pp. 17–24). IEEE.
26. Kaswan, K.S., Gautam, R. and Dhatteval, J.S., 2022. Introduction to DSS system for smart cities. In *Decision Support Systems for Smart City Applications* (pp. 53–76). Wiley Online Library.
27. Jara, A.J., Sun, Y., Song, H., Bie, R., Genouod, D. and Bocchi, Y., 2015, March. Internet of things for cultural heritage of smart cities and smart regions. In *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops* (pp. 668–675). IEEE.
28. Logota, E., Mantas, G., Rodriguez, J. and Marques, H., 2015. Analysis of the impact of denial of service attacks on centralized control in smart cities. In *Wireless Internet: 8th International Conference, WICON 2014, Lisbon, Portugal, November 13–14, 2014, Revised Selected Papers 8* (pp. 91–96). Springer International Publishing.

29. Tsai, D.R., Tai, W.P. and Chang, C.F., 2003, October. A hybrid intelligent intrusion detection system to recognize novel attacks. In *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings* (pp. 428–434). IEEE.
30. Kim, G., Lee, S. and Kim, S., 2014. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications*, 41(4), pp. 1690–1700.
31. Ayo, F.E., Folorunso, S.O., Abayomi-Alli, A.A., Adekunle, A.O. and Awotunde, J.B., 2020. Network intrusion detection based on deep learning model optimized with rule-based hybrid feature selection. *Information Security Journal: A Global Perspective*, 29(6), pp. 267–283.
32. Abadeh, M.S., Habibi, J. and Lucas, C., 2007. Intrusion detection using a fuzzy genetics-based learning algorithm. *Journal of Network and Computer Applications*, 30(1), pp. 414–428.
33. Moustafa, N. and Slay, J., 2015, November. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In *2015 Military Communications and Information Systems Conference (MilCIS)* (pp. 1–6). IEEE.
34. Yassin, W., Udzir, N.I., Muda, Z. and Sulaiman, M.N., 2013. Anomaly-based intrusion detection through k-means clustering and Naives Bayes classification. In *Proceedings of the 4th International Conference on Computing and Informatics (ICOCI 2013), 28–30 August, 2013 Sarawak, Malaysia, Universiti Utara Malaysia*. (<http://www.uum.edu.my>).
35. Aghaei, E. and Serpen, G., 2017. Ensemble classifier for misuse detection using N-gram feature vectors through operating system call traces. *International Journal of Hybrid Intelligent Systems*, 14(3), pp. 141–154.
36. Subba, B., Biswas, S. and Karmakar, S., 2017, November. Host based intrusion detection system using frequency analysis of n-gram terms. In *TENCON 2017–2017 IEEE Region 10 Conference* (pp. 2006–2011). IEEE.
37. Xie, M., Hu, J. and Slay, J., 2014, August. Evaluating host-based anomaly detection systems: Application of the one-class SVM algorithm to ADFA-LD. In *2014 11th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)* (pp. 978–982). IEEE.
38. Hall, J., Barbeau, M. and Kranakis, E., 2005, August. Anomaly-based intrusion detection using mobility profiles of public transportation users. In *WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications, 2005* (Vol. 2, pp. 17–24). IEEE.
39. Tong, X., Wang, Z. and Yu, H., 2009. A research using hybrid RBF/Elman neural networks for intrusion detection system secure model. *Computer Physics Communications*, 180(10), pp. 1795–1801.
40. Tang, M., Alazab, M., Luo, Y. and Donlon, M., 2018. Disclosure of cyber security vulnerabilities: Time series modelling. *International Journal of Electronic Security and Digital Forensics*, 10(3), pp. 255–275.
41. Smys, S., Basar, A. and Wang, H., 2020. Hybrid intrusion detection system for internet of things (IoT). *Journal of ISMAC*, 2(4), pp. 190–199.
42. Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C. and Bellekens, X., 2021, January. Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset). In *Selected Papers from the 12th International Networking Conference: INC 2020* (pp. 73–84). Springer International Publishing.
43. Hindy, H., Bayne, E., Bures, M., Atkinson, R., Tachtatzis, C. and Bellekens, X., 2021, January. Machine learning based IoT intrusion detection system: An MQTT case

- study (MQTT-IoT-IDS2020 dataset). In *Selected Papers from the 12th International Networking Conference: INC 2020* (pp. 73–84). Springer International Publishing.
44. Khan, M.A., Khan, M.A., Jan, S.U., Ahmad, J., Jamal, S.S., Shah, A.A., Pitropakis, N. and Buchanan, W.J., 2021. A deep learning-based intrusion detection system for MQTT enabled IoT. *Sensors*, 21(21), p. 7016.
 45. Hindy, H., Tachtatzis, C., Atkinson, R., Bayne, E. and Bellekens, X., 2020. MQTT-IoT-IDS2020: MQTT internet of things intrusion detection dataset. *IEEE Dataport* [Online]. Available: <https://iee-dataport.org/open-access/mqtt-iot-ids2020-mqtt-internet-things-intrusion-detection-dataset>.

10 Cyber Security for Edge/Fog Computing Applications

Hanane Lamaazi

10.1 INTRODUCTION

Edge/fog computing has emerged as a promising solution to overcome centralized platform challenges, such as limited bandwidth and high response time, by placing the computing resources closer to end users [1]. However, the distributed nature of edge/fog computing platforms introduces new challenges related to the security of infrastructure as well as data protection [2]. The diversity of deployed IoT devices used to sense data and transmission technologies produces an inconsistency of standardization, increasing the criticality of providing optimal and common security controls and services. Existing and emerging attacks target edge/fog computing for many reasons, including their closeness to end users [3], local data storing and processing, and lack of normalized security solutions. The attacks can cause serious damage, such as data breaches, physical destruction, reputation degradation, physical harm, financial loss, etc.

Furthermore, deploying edge/fog computing in critical and time-sensitive applications such as healthcare and transportation requires effective security controls and services, where a cyber attack could have serious consequences. In addition, best practices, security policies, and recommendations should be part of the security plan for more effectiveness.

The main purpose of this chapter is to provide an extensive overview of cyber security for edge/fog computing applications. It explores cyber security's importance and highlights potential threats and risks and their impact on edge/fog computing. Also, it presents a set of existing and emerging technologies and techniques for cyber security, such as blockchain and artificial intelligence. It provides insights into the impact of future developments and directions effective to secure edge/fog computing systems. This chapter also highlights the importance of standardization and regulation in cyber security for edge/fog computing. Using a unified approach to cyber security while considering the distributed nature of edge/fog platforms can guarantee that all edge/fog devices are secured uniformly.

This chapter:

- Provides a deep study of cyber security for edge/fog computing applications, including the emerging threats and risks and their impact on these systems.

- Examines some case studies of successfully implemented cyber security solutions in edge/fog computing applications.
- Discusses the importance of non-technical security solutions.
- Sheds light on various defense systems and platforms used for cyber security in edge/fog computing.
- Highlights some emerging technologies, techniques, and best practices for edge/fog computing cyber security.
- Provides some future directions

10.2 FUNDAMENTALS EDGE/FOG COMPUTING AND CYBER SECURITY

It is important to understand the characteristics and functionalities of edge/fog computing and the need to secure these entities that constitute an attractive target for cyber attacks.

Edge/fog computing was developed to offload the cloud and overcome some of its shortcomings. With the increase of connected devices, platforms, and users, the amount of data increases, and processing it locally within the cloud becomes more complex. Thus shifting from a large-scale centric platform for big data processing to diversified and distributed data storage with fast response and advanced computing capabilities has become a requirement [4]. Edge/fog computing inherited the benefits of cloud computing while bringing new advantages. It reduces the response time, and the data computation complexity allows local processing and minimizes the amount of network traffic, etc. Compared to cloud computing, edge/fog computing systems are constrained resources with limited computing capabilities. However, their heterogeneity makes them optimal for handling different tasks with different requirements, and their distribution in other locations makes them closer to the end users [4]. As mentioned previously, edge/fog computing can locally process the data; this means it can interact with the end user without the cloud's intervention while communicating with the cloud to collect or store the data.

In terms of security, cloud computing faces several issues and challenges due to its centralized nature. The data is stored with a third-party provider, while it can be accessed through the Internet; this limits the control and visibility of the data and exposes it to theft, corruption, and falsification. Edge/fog computing reduces the security issues raised with the cloud. Placing edge/fog computing close to the end user reduces response time, and the chances that the data get intercepted become lower. Also, the data distribution among different edge/fog servers ensures the continuity of data processing; even with the destruction of one server, the others remain available. Considering their unique architecture and role as an intermediate layer between the cloud and end user, edge/fog computing platforms require strong cyber security systems that protect the infrastructure and the collected and stored data. Edge/fog computing can be a target for large attacks, threats, and risks for a set of reasons:

- **Distributed Systems:** Edge/fog computing systems are highly distributed and connected to numerous devices and platforms, making them an interesting motif for attackers to raise a mass attack by gaining access to one of the edge/fog servers or access to the cloud, affecting all the connected edge/fog servers.
- **Data Storage:** All the cyber attacks related to sensitive information are applied in the case of edge/fog computing systems. The limited amount of data processed locally in the edge/fog systems and quickly shared with end users helps to access the information and spread the falsified data in response.
- **End User:** The types of edge/fog computing systems users vary according to the application domain, assigned tasks, and user status. They can be workers, employees, customers, contractors, or vendors. This not only forces edge/fog computing systems to face external threats, but insiders with authorized access to the systems can also raise them. The risk of causing damage or data breaches unintentionally or intentionally increases.
- **Resource Constraints:** Implementing powerful security controls requires high storing and computing capability. However, with the limited resources of edge/fog computing systems in terms of network bandwidth, computing power, and storage, detecting or preventing cyber attacks becomes very challenging.
- **Connectivity Lifetime:** Edge/fog computing systems must operate continuously to provide real-time responses. This increases the chance of successful penetrations by attackers and then their creating an interruption of network connection.

Table 10.1 presents the different characteristics of edge/fog computing, its benefits, and its related threats.

TABLE 10.1
Benefits and Threats Related to Edge/Fog Computing Characteristics

Characteristics	Benefit	Related Threat
Distributed systems	Parallel processing, which reduces computation time	Spread of attacks
Data storage	Facilitate data recovery	Easy access and falsification of a small amount of data
End user	Real-time interaction	Can be an insider or an outsider threat
Resource constraints	Preserve resource consumption	Limit security controls efficiency
Connectivity lifetime	Ensure cooperation and continuous availability	Attackers have more time to raise an attack

10.3 CYBER SECURITY THREATS, VULNERABILITIES, AND RISKS IN EDGE/FOG COMPUTING

As with any technology, edge/fog computing systems can face attacks that can exploit some vulnerabilities to penetrate the system and data. They can attain the confidentiality, integrity, and availability of stored and shared data [5, 6]. In this section, a set of common threats and risks related to cyber attacks on edge/fog computing systems are described.

- **Malware Attacks:** Edge/fog computing systems can be vulnerable to malware attacks such as worms, viruses, and Trojan horses that use malicious software to affect devices critical to the systems' operation [7]. They may manipulate system performances, steal data, or launch other attacks. Also, they can spread quickly through the network, where multiple devices and applications are affected.
- **Ransomware Attacks:** Ransomware attacks can be destructive to edge/fog computing systems, particularly for time-sensitive data, where attackers can encrypt it and then ask for payment to provide the decryption key. This can disrupt the system's availability, leading to significant consequences.
- **Insider Threats:** Insider threats refer to attacks or security breaches from within an organization where authorized users misuse their privilege and bypass security measures to access edge/fog systems. They can intentionally or unintentionally cause significant damage to data and infrastructures or disrupt system availability.
- **Denial-of-Service (DoS):** Attacks involve overloading edge/fog computing systems with requests, causing the system to become unavailable to legitimate users. This can cause a disruption of operations and data that requires real-time processing and communication.
- **Supply Chain Attacks:** Supply chain attacks involve fabrication threats. Vendors or third-party suppliers of a target system can gain unauthorized access to software or hardware components of an edge/fog computing system, allowing manipulation of a system behavior or stalling sensitive data stored in the servers.
- **Lack of Standardization:** Edge/fog computing environments may use inconsistent protocols and security measures. Without standardization, the risk of security breaches and loss of integrity of edge/fog computing systems becomes high.
- **Human Error:** Human error, such as configuration mistakes, poor password management, and weak programs, can make edge/fog computing systems vulnerable to cyber attacks.
- **Interception Attacks:** It's an attack on confidentiality [8]. It involves eavesdropping on communication, wiretapping telecommunication between devices in edge/fog computing systems, and copying programs used to access sensitive data or launch further attacks.
- **Man-in-the-Middle (MitM) Attacks:** In the context of edge/fog computing systems, MitM attacks can intercept data shared between IoT devices, edge/fog servers, and cloud servers [9].

- **IoT-Specific/IoT Botnets Attacks:** Edge/fog computing systems collect the data sensed by IoT devices. A set of attacks can target those devices and launch a range of attacks, such as spoofing, replay, firmware, and command injection attacks.
- **Social Engineering:** Edge/fog computing environments can be a target for social engineering attacks. Due to the unfamiliarity of users with security protocol, attackers can gain access to IoT devices and steal the sensed data. It includes pretexting, phishing, and baiting.
- **Lack of Visibility:** Edge/fog computing systems are moving targets often located in different locations and devices. They may lack visibility, making detecting and responding to cyber threats difficult and making it difficult for organizations to have full visibility and control over their systems.
- **Lack of Scalability:** Edge/fog computing systems often need to satisfy scalability requirements by quickly and dynamically meeting the requested changes. Due to this dynamicity, implementing consistent security measures and protocols becomes difficult.
- **Lack of Expertise:** Edge/fog computing systems require specialized qualifications and expertise to implement and manage security controls effectively.
- **Shadow IT:** In edge/fog computing systems, using unauthorized or unverified devices or software may not be properly vetted for security risks and may introduce a set of security vulnerabilities and weaknesses.
- **Interoperability:** Deploying heterogeneous devices forces edge/fog computing environments face interoperability challenges. Thus maintaining the security and integrity of edge/fog computing environments may be critical.
- **Regulatory Compliance:** Edge/fog computing systems can be subject to different data protection and privacy regulations. Failure to follow these regulations leads to significant reputational and financial damage.
- **Misuse of Encryption:** Encryption is important for ensuring data confidentiality and integrity in edge/fog computing systems. However, the lack of encryption or inappropriate encryption can cause data interception or theft.
- **Misconfiguration of Access Controls:** The misconfiguration of access controls, such as multifactor authentication, passwords, and role-based access control, can make edge/fog computing systems subject to unauthorized access and data breaches.
- **Physical Security Risks:** Edge/fog computing systems are integrated into physical devices and infrastructure such as servers, mobile devices, sensors, etc. These physical devices can be damaged, destroyed, or tampered with. Physical attacks can compromise the integrity and security of the whole system.

Figure 10.1 presents the different existing risks according to their related categories: threat, vulnerability, and asset

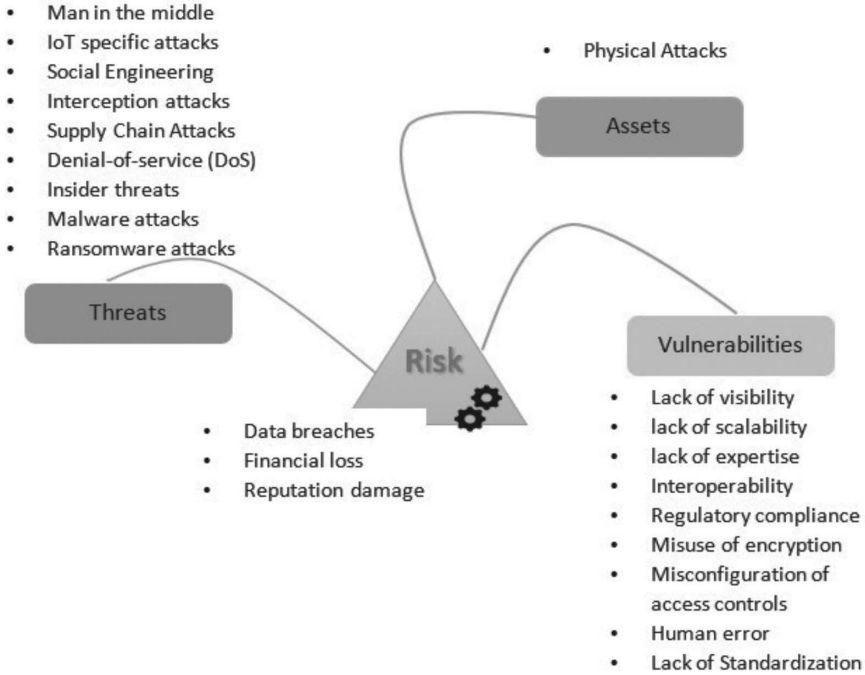


FIGURE 10.1 Risk related to edge/fog computing systems.

10.4 IMPACT OF CYBER ATTACKS ON EDGE/ FOG COMPUTING APPLICATIONS

Cyber attacks can significantly affect edge/fog computing applications. It causes data breaches and services disruption, possesses unauthorized access, manipulates the systems, and leads to serious financial and reputational damage. A set of the common impact of cyber attacks on edge/fog applications is described next.

- **Data Breaches:** In edge/fog computing systems, the data is distributed, stored, and processed on multiple servers. Storing the data and transmitting it without protection make it an attractive target for cyber attackers, which can lead to significant personal, financial, and reputational damage. Also, detecting those breaches may be more difficult due to the distributed nature of edge/fog computing systems.
- **Service Disruptions:** Cyber attacks can target the edge/fog system’s availability by overloading the system causing device downtime, service disruption, and productivity loss.
- **Malware Infections and Unauthorized Access:** Edge/fog systems provide a large surface for malware has been developed for more than 50% of the targeted IoT devices. Having penetrated the edge/fog systems, the malware, such as viruses, adware, and spyware, leads to serious damage to system operations. It can allow unauthorized access to system

resources, causing frequent crashing, stealing of sensitive information, and financial loss.

- **Reputational/Financial Damage:** Attacking edge/fog computing applications can cause financial and reputational losses. Unauthorized access to sensitive information and services can affect user trust and confidence. This reduces the reputation of the service providers, leading to financial and business failure.
- **Cybersecurity Costs:** Addressing Cyber attacks on edge/fog computing applications is not an easy task and requires high costs that include service and controls implementation, cyber security experts, assessment, and auditing.
- **Supply Chain Disruptions:** Various industries rely on edge/fog computing applications. Attacking supply chains, particularly logistics systems, can hold up goods delivery and services, causing serious economic loss.
- **Social Impacts:** Cyber attacks on edge/fog computing applications can also have social impacts. They can be manipulated and used to spread fake news and false alerts and to induce wrong decision making. This could expose users' lives and well-being to high risks and negative social problems.

10.5 CYBER SECURITY MEASURES AND BEST PRACTICES FOR EDGE/FOG COMPUTING

10.5.1 PROACTIVE CYBER SECURITY STRATEGY

Proactive cyber security strategies are crucial for protecting edge/fog computing systems from cyber attacks [10]. These strategies cover regulations and standards, Auditing, employee training, and data recovery, as presented in Figure 10.2 and explained next.

- **Regular Security Audits:** Securing edge/fog systems requires continuous assessment and audit. This helps identify vulnerabilities, standards violations, and emerging threats and remediates them before threat agents exploit them. A set of techniques can be used to apply this assessment and auditing, such as penetration testing, threat analysis, patch remediation, certification verification, and compliance with regulations and standards such as ISO 27001, HIPAA, GDPR, etc. [11].
- **Employee Training:** Some threats can be caused accidentally by insiders due to a lack of knowledge. Thus training employees is an important element of any effective cyber security strategy. Deploying employees with high and updated expertise reduces the probability that a vulnerability can be committed when designing, implementing, or configuring a system.
- **Use of Advanced Security Technologies:** As sensitive entities, edge/fog computing systems need advanced protection and security depth, which should include multilayer security controls such as firewalls, intrusion detection and prevention systems, and security information and event management (SIEM) systems. Also, deploying new AI and machine learning technologies helps detect real-time attacks with fast response time [12].

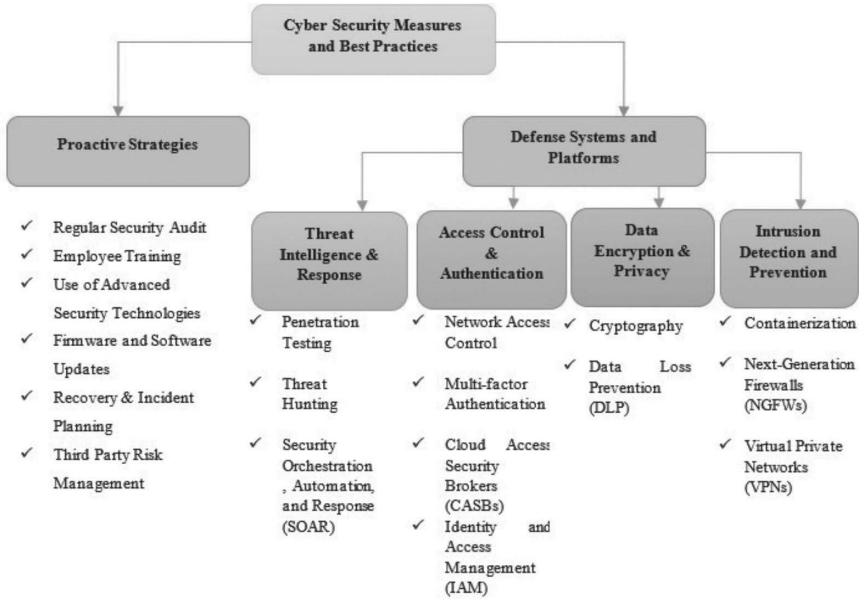


FIGURE 10.2 Cyber security measures and best practices.

- **Firmware and Software Updates:** Patch and bug remediation and software and firmware updates are essential to keep the edge/fog systems operating properly. This improves their functionalities and features and fixes performance issues. These updates should be processed on the edge/fog systems and on the interconnected IoT devices to avoid any incoming problems.
- **Recovery and Incident Planning:** Edge/fog systems should be resilient to any sudden event, whether a natural disaster, attack, internal threat, etc. Using recovery and continuous planning is a crucial element in cyber security. This includes the development of backup and recovery procedures, detection, isolation, and recovery from discovered cyber attacks, as well as notification protocols to alert users about the incident.
- **Third-Party Risk Management:** Deploying third-party risk management ensures that the vendors of hardware and software components follow the cyber security norms and standards and that no violations of those norms are reported [11].

10.5.2 OTHER DEFENSE SYSTEMS AND PLATFORMS

In addition to the proactive cyber security strategies mentioned earlier, several other defense systems and platforms can be used to protect edge/fog computing systems against cyber attacks.

10.5.2.1 Access Control and Authentication

- **Network Access Control (NAC):** NAC is a security measure that allows control access to edge/fog systems by enforcing policies that authorize

only recognized devices to connect to the systems and to share information or receive tasks for the sensing process [13]. Limiting access to edge/fog systems reduces the risk that a malicious user raises an attack or steals information.

- **Multifactor Authentication (MFA):** MFA is the initial element of access control where users must provide multiple forms of authentication to access edge/fog applications. MFA helps not only to verify the users but also to track abnormal activities by clearly identifying the threat sources.
- **Cloud Access Security Brokers (CASBs):** Edge/fog systems interact with cloud computing to share collected and processed data or to receive tasks from the cloud to execute them. Securing cloud systems is a key edge/fog security network component [14]. Integrating a CASB between cloud service consumer and provider helps enforce regulatory compliance, protect the data, identify the risk, and optimize cloud usage across applications and devices [15].
- **Identity and Access Management (IAM):** IAM solutions are an important element of security strategy. It provides a centralized framework of technologies and policies for managing user identities and access privileges. It includes user provisioning, MFA, identity analytics, single sign-on establishment, zero-trust policy implementation, etc. Using IAM with edge/fog systems can enforce strong access controls and reduce the risk of insider threats.

10.5.2.2 Data Encryption and Privacy

- **Cryptography:** Cryptography is crucial security control required to secure communication and shared data. It helps to hide the content of the information using a key that can be used for encryption at the sender level and for decryption at the receiver level [16]. It takes different forms, such as symmetric and asymmetric encryptions and hash functions. Integrating cryptography in edge/fog systems protects the data even if cyber attackers intercept it.
- **Data Loss Prevention (DLP):** DLP is the measure of preventing any unauthorized disclosure, destruction, or exfiltration of sensitive data such as personnel credential information or financial data. By implementing DLP practice within edge/fog computing systems, the sensed and processed data remains protected from breaches and other types of cyber attacks that could result in the loss of sensitive data.

10.5.2.3 Intrusion Detection and Prevention

- **Containerization:** This involves deploying an isolated software or process that packs a code with all needed files and libraries that can be run on any system or infrastructure [17]. This addresses the problem of compatibility that existed with traditional applications. The risk of fabrication attacks is reduced by containerizing edge/fog computing applications and processes.
- **Next-Generation Firewalls (NGFWs):** NGFWs offer advanced security features and capabilities over those of traditional firewalls, such as deep packet inspection, application-level awareness, and intrusion prevention.

NGFWs can be deployed on both sides between edge/fog systems and cloud or between edge/fog systems and IoT devices [18, 19]. This provides more protection against modern and advanced cyber threats.

- **Virtual Private Networks (VPNs):** VPNs are useful for edge/fog systems and IoT devices, especially with unsecured networks. VPNs provide anonymity and security to users when connected to web-based sites and services. They hide users' IP addresses and allow communication between users and edge/fog systems using a secured tunnel.

10.5.3 THREAT INTELLIGENCE AND RESPONSE

- **Penetration Testing:** Penetration testing is a good practice to evaluate the effectiveness of the control. It involves simulating a cyber attack against edge/fog systems to identify potential weaknesses and vulnerabilities. This helps to address those vulnerabilities before being exploited by cyber attackers.
- **Threat Hunting:** Threat hunting is a proactive defense method to identify potential cyber threats or non-remediated threats before they can disrupt the system. This can protect edge/fog systems from ongoing threats and respond effectively and quickly to any incidents that can occur over time.
- **Security Orchestration, Automation, and Response (SOAR):** SOAR technology provide a centralized platform that coordinates, automates, and executes tasks while managing workflows of security incidents across a system. This helps edge/fog systems to easily handle security routines such as threat detection and response action and to protect the systems from future incidents.

10.6 NEW TECHNOLOGIES AND TECHNIQUES FOR CYBER SECURITY IN EDGE/FOG COMPUTING

The continuous growth of edge/fog computing deployment involves integrating emergent technologies and techniques to improve cyber security in these environments [12, 20]. Here are some examples of the most used technologies:

- **Blockchain:** Blockchain technology can be used to secure edge/fog computing applications by providing a decentralized control of data and by making it tamper-proof for storing, verifying, and preserving its consistency [21]. It can enable secure peer-to-peer communication and improve overall system resiliency [22].
- **Machine Learning:** Deploying machine learning algorithms in edge/fog computing environments improves the real-time response time of the detection and prevention of cyber attacks. Using predefined features extracted from historical data, these algorithms can learn from patterns and behavior to identify abnormal activities and user misbehaving and notify the administrators of potential threats [23, 24].

- **Zero-Trust Architecture:** Zero-trust architecture is an approach used to enforce access policies that require strict authentication and authorization for every access attempt made by users, applications, and devices. This approach is an effective security measure for edge/fog computing environments where devices and users may be out of the area of interest [25].
- **Virtualization:** Virtualization technology creates virtual versions of particular entities, such as servers, storage devices, networks, etc., deployed on a single physical device [26]. These virtual machines (VMs) can run simultaneously and are isolated and secured through encryption and access privileges, which protect edge/fog systems from cyber attacks [27].

10.7 DISCUSSION AND FUTURE DIRECTIONS

Edge/fog computing brings many benefits and allows us to overcome challenges related to centralized platforms. Nowadays, it is widely used in a set of application domains and industries. Ensuring the security of edge/fog computing systems is one of the main challenges that ongoing development and research in cyber security are interested in.

Here are some potential areas for future research:

- Improve the complexity of existing defense systems and platforms or develop more advanced ones for edge/fog computing that can better detect and respond to emerging vulnerabilities and threats
- Investigate and Integrate new technologies and techniques such as blockchain, artificial intelligence, and quantum computing to secure edge/fog computing applications.
- Investigate the compliance and regulatory requirements for cyber security in edge/fog computing, and develop best practices and effective strategies for compliance with these requirements.
- Develop new educational and training programs for IT professionals and end users to increase their knowledge, understanding, and awareness of the importance of cyber security in edge/fog computing.

10.8 CONCLUSION

Edge/fog computing is an emerging technology that has helped overcome centralized platform challenges and that has been integrated into various industries to collect, process, and store data. Placed close to the data source, edge/fog computing offer an optimal solution to handle complex tasks promptly. Edge/fog computing is also used to ensure multilevel cooperation between IoT-to-edge or edge-to server entities and to propagate information accordingly. These characteristics make edge/fog computing vulnerable to cyber crimes that can manipulate systems and the users in order to gain unauthorized access and to corrupt, disrupt, or exfiltrate the data. To protect edge/fog computing from malicious activities and attacks, it is important to understand the concept of edge/fog deployment and cyber security. Securing a system should consider technical and non-technical solutions. This chapter presents a comprehensive overview of edge/fog computing cyber security. It explored common

threats and risks, integration of emerging technologies and techniques, standardization and regulations, and defense systems and platforms. Also, it presented some case studies of security implementations developed for edge/fog computing. It is important to consider the risks relate to target edge/fog computing systems, to evaluate and rate them, to develop optimal security solutions, and to implement the most effective measures and controls. This helps to protect infrastructure, devices, and data. This chapter also provided some guidelines and best practices that help reduce vulnerabilities and guarantee the data's confidentiality, integrity, and availability.

REFERENCES

- [1] H. Lamaazi, R. Mizouni, H. Otrok, S. Singh, and E. Damiani, "Trust-3DM: Trustworthiness-Based Data-Driven Decision-Making Framework Using Smart Edge Computing for Continuous Sensing," *IEEE Access*, vol. 10, pp. 133095–133108, 2022, doi:10.1109/ACCESS.2022.3231549.
- [2] H. Lamaazi, R. Mizouni, S. Singh, and H. Otrok, "A Mobile Edge-Based CrowdSensing Framework for Heterogeneous IoT," *IEEE Access*, vol. 8, pp. 207524–207536, 2020, doi:10.1109/ACCESS.2020.3038249.
- [3] M. Laroui, B. Nour, H. Mounsla, M. A. Cherif, H. Afifi, and M. Guizani, "Edge and fog Computing for IoT: A Survey on Current Research Activities & Future Directions," *Computer Communications*, vol. 180. Elsevier B.V., pp. 210–231, Dec. 01, 2021, doi:10.1016/j.comcom.2021.09.003.
- [4] H. G. Abreha, M. Hayajneh, and M. A. Serhani, "Federated Learning in Edge Computing: A Systematic Survey," *Sensors*, vol. 22, no. 2. MDPI, Jan. 01, 2022, doi:10.3390/s22020450.
- [5] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security," *Internet of Things*, p. 100759, Mar. 2023, doi:10.1016/j.iot.2023.100759.
- [6] R. Roman, J. Lopez, and M. Mambo, "Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, Jan. 2018, doi:10.1016/j.future.2016.11.009.
- [7] A. Shakarami, H. Shakarami, M. Ghobaei-Arani, E. Nikougoftar, and M. Faraji-Mehmandar, "Resource Provisioning in Edge/Fog Computing: A Comprehensive and Systematic Review," *Journal of Systems Architecture*, vol. 122. Elsevier B.V., Jan. 01, 2022, doi:10.1016/j.sysarc.2021.102362.
- [8] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues," *IEEE Access*, vol. 6, pp. 18209–18237, Mar. 2018, doi:10.1109/ACCESS.2018.2820162.
- [9] P. Y. Zhang, M. C. Zhou, and G. Fortino, "Security and Trust Issues in Fog Computing: A Survey," *Future Generation Computer Systems*, vol. 88, pp. 16–27, Nov. 2018, doi:10.1016/j.future.2018.05.008.
- [10] R. Das and M. M. Inuwa, "A Review on Fog Computing: Issues, Characteristics, Challenges, and Potential Applications," *Telematics and Informatics Reports*, vol. 10, p. 100049, Jun. 2023, doi:10.1016/j.teler.2023.100049.
- [11] W. Zhang, H. Jiao, Z. Yan, X. Wang, and M. K. Khan, "Security Analysis and Improvement of a Public Auditing Scheme for Secure Data Storage in Fog-to-Cloud Computing," *Computers & Security*, vol. 125, Feb. 2023, doi:10.1016/j.cose.2022.103019.
- [12] S. Iftikhar et al., "AI-Based Fog and Edge Computing: A Systematic Review, Taxonomy and Future Directions," *Internet of Things (Netherlands)*, vol. 21. Elsevier B.V., Apr. 01, 2023, doi:10.1016/j.iot.2022.100674.

- [13] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "Insights into Security and Privacy Towards Fog Computing Evolution," *Computers and Security*, vol. 120. Elsevier Ltd, Sep. 01, 2022, doi:10.1016/j.cose.2022.102822.
- [14] K. A. Torkura, M. I. H. Sukmana, T. Strauss, H. Graupner, F. Cheng, and C. Meinel, "CSBAuditor: Proactive Security Risk Analysis for Cloud Storage Broker Systems," in *NCA 2018–2018 IEEE 17th International Symposium on Network Computing and Applications*, Institute of Electrical and Electronics Engineers Inc., Nov. 2018, doi:10.1109/NCA.2018.8548329.
- [15] C. Liu, G. Wang, P. Han, H. Pan, and B. Fang, "A Cloud Access Security Broker Based Approach for Encrypted Data Search and Sharing," in *2017 International Conference on Computing, Networking and Communications, ICNC 2017*, Institute of Electrical and Electronics Engineers Inc., Mar. 2017, pp. 422–426, doi:10.1109/ICCNC.2017.7876165.
- [16] R. Rezapour, P. Asghari, H. H. S. Javadi, and S. Ghanbari, "Security in Fog Computing: A Systematic Review on Issues, Challenges and Solutions," *Computer Science Review*, vol. 41. Elsevier Ireland Ltd, Aug. 01, 2021, doi:10.1016/j.cosrev.2021.100421.
- [17] Y. Liu, D. Lan, Z. Pang, M. Karlsson, and S. Gong, "Performance Evaluation of Containerization in Edge-Cloud Computing Stacks for Industrial Applications: A Client Perspective," *IEEE Open Journal of the Industrial Electronics Society*, vol. 2, pp. 153–168, 2021, doi:10.1109/OJIES.2021.3055901.
- [18] B. Soewito and Charlie E. Andhika, "Next Generation Firewall for Improving Security in Company and IoT Network," in *International Seminar on Intelligent Technology and Its Applications (ISITIA)*, IEEE, 2019, p. 450, doi:10.1109/ISITIA.2019.8937145.
- [19] K. Neupane, R. Haddad, and L. Chen, "Next Generation Firewall for Network Security: A Survey," in *SoutheastCon 2018*, St. Petersburg, FL, 2018, pp. 1–6, doi:10.1109/SECON.2018.8478973.
- [20] R. Singh and S. S. Gill, "Edge AI: A Survey," *Internet of Things and Cyber-Physical Systems*, vol. 3. KeAi Communications Co., pp. 71–92, Jan. 01, 2023, doi:10.1016/j.iotcps.2023.02.004.
- [21] S. A. Bhat, I. B. Sofi, and C. Y. Chi, "Edge Computing and Its Convergence with Blockchain in 5g and Beyond: Security, Challenges, and Opportunities," *IEEE Access*, vol. 8, pp. 205340–205373, 2020, doi:10.1109/ACCESS.2020.3037108.
- [22] H. Xue, D. Chen, N. Zhang, H. N. Dai, and K. Yu, "Integration of Blockchain and Edge Computing in Internet of Things: A Survey," *Future Generation Computer Systems*, 2022, doi:10.1016/j.future.2022.10.029.
- [23] K. Sha, T. A. Yang, W. Wei, and S. Davari, "A Survey of Edge Computing-Based Designs for IoT Security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 195–202, May 2020, doi:10.1016/j.dcan.2019.08.006.
- [24] L. Coppolino, S. D. Antonio, G. Mazzeo, and L. Romano, "A Comprehensive Survey of Hardware-Assisted Security: From the Edge to the Cloud," 2019, doi:10.1016/j.iot.2019.10.
- [25] P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi:10.1109/ACCESS.2023.3248622.
- [26] F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. B. Kent, and S. Hakak, "Cloud Computing Security: A Survey of Service-Based Models," *Computers & Security*, vol. 114, Mar. 2022, doi:10.1016/j.cose.2021.102580.
- [27] R. Singh, R. Sukapuram, and S. Chakraborty, "A Survey of Mobility-Aware Multi-Access Edge Computing: Challenges, Use Cases and Future Directions," *Ad Hoc Networks*, vol. 140. Elsevier B.V., Mar. 01, 2023, doi:10.1016/j.adhoc.2022.103044.

11 Cyber Attacks Against Intelligent Transportation Systems

*Muhammad Usama, Ubaid Ullah,
and Aththasham Sajid*

11.1 INTRODUCTION

Smart cities are a novel idea for urban planners, with new programs like the U.S. Department of Mobility's Smart City Challenge encouraging more effective urban mobility [1, 2]. To improve operational efficiency, intelligent cities use networked technologies to collect real-time data, analyze it, and make preventative and adaptive decisions [3]. Intelligent transportation systems (ITS) are generally used to describe innovative transportation systems. ITSs are the coordinated use of information processing, management, and communications technology in the transportation system. Computers, electronics, satellites, and sensors are used in the execution of transportation operations for traffic management, journey planning, and vehicle control. There are many benefits, but enhanced ease, efficacy, and safety are the most important ones [4]. An ITS aims to provide better services for drivers and commuters in transportation networks [5]. By integrating modern technologies into transportation infrastructure and vehicles, an ITS seeks to increase transportation efficiency and safety. An ITS provides real-time data and information about traffic conditions, weather, road conditions, and other factors that influence the transportation system in order to assist transport operators and users in making better choices [6].

The ITS movement began in the early 1970s when academics and decision makers looked into technology to increase transit efficiency and safety [7]. The first cutting-edge traffic control and intelligent vehicle systems were developed at the outset of the ITS revolution [8]. Several ITS pilot projects emphasizing advanced traveler information systems, real-time traffic management and control, and electronic toll collection were launched in the 1980s in Europe and the United States [9, 10]. All current ITS projects need vehicular ad hoc networks (VANET), an essential component. Nodes (vehicles) in the VANET occasionally trade short messages known as beacons. Important information about the surroundings and moving vehicles, such as direction, acceleration, speed, road conditions, weather conditions, and more, is stored in the signals. User identity protection, interruptions, multi-hop communication, and considerable heterogeneity are just a few of the difficulties associated with wireless one-hop communication for vehicle connectivity (depending on whether the

cars are congested in a big city or a suburban area). Network security is the main emphasis of ITS cyber security research [11, 12].

Not all ITS components are at risk, including VANETs. A system as complex as the ITS necessitates protection everywhere. Attempts to automate transit have led to the use of fog and cloud computing, artificial intelligence, and machine learning in the ITS. The difficulty of ensuring cyber security may severely hamper the practical application of completely automated vehicles. Don't undervalue the non-technical component of ITS security. It is reflected in the thoughtful analysis of authorization policy, standards creation, governance, policy, regulation, awareness, and education [13]. The ITS has become an increasingly popular solution for modern-day transportation issues. Employing ITSs has numerous advantages, the primary of which are time and energy savings. It is estimated that using ITSs can reduce the time spent driving by 40–70%, thereby reducing energy consumption [14]. This is a significant advantage, as it not only saves time for individuals but also helps in reducing the carbon footprint. Additionally, using ITSs can lead to a 30–50% reduction in exhaust emissions, resulting in a healthier and more sustainable environment.

Moreover, ITSs can also help in reducing road fleet management expenses. With ITSs, monitoring and managing vehicles and equipment have become more efficient, leading to cost savings [15]. This can be especially beneficial for organizations with a large fleet of vehicles. By employing ITSs, they can reduce their expenses and optimize their resources. The ITS is a rapidly growing field, with ongoing research and development focused on improving transportation safety, efficiency, and sustainability [16]. Major ITS applications include advanced traffic management systems, electronic toll collection, intelligent public transportation systems, and connected and automated vehicles [17].

Cyber attacks' danger increases as more vehicles are interconnected thanks to innovations like the ITS and vehicle ad hoc networks (VANET). To address this problem, a list of the most significant cyber threats to such networks was compiled after a review of numerous sources describing key information security issues. These dangers include broadcast tampering, which involves the modification of messages sent over the network, potentially causing collisions or other dangerous situations [18]. Another threat is routing, which attackers can employ to cause traffic congestion or reroute vehicles to undesirable locations [19, 20]. Traffic analysis is another danger allowing attackers to obtain sensitive information about the network and its users. Jamming, the intentional disruption of wireless signals, is also a concern as it can render the network unusable [21]. Track and GPS spoofing/position faking are additional risks that can compromise the privacy and safety of vehicle occupants. Those involved in designing and implementing VANET/ITS networks must be aware of these dangers and take appropriate measures to mitigate them. Based on our review of the numerous sources covering key information security subjects in VANET/ITS networks, a list of the top cyber threats confronting such networks was created [22–24].

This chapter discusses various types of cyber attacks that can occur in ITSs. It also explores the potential consequences of such attacks, including the disruption of critical transportation infrastructure and the compromise of passenger safety. Additionally, it has examined the current state of cyber security measures within

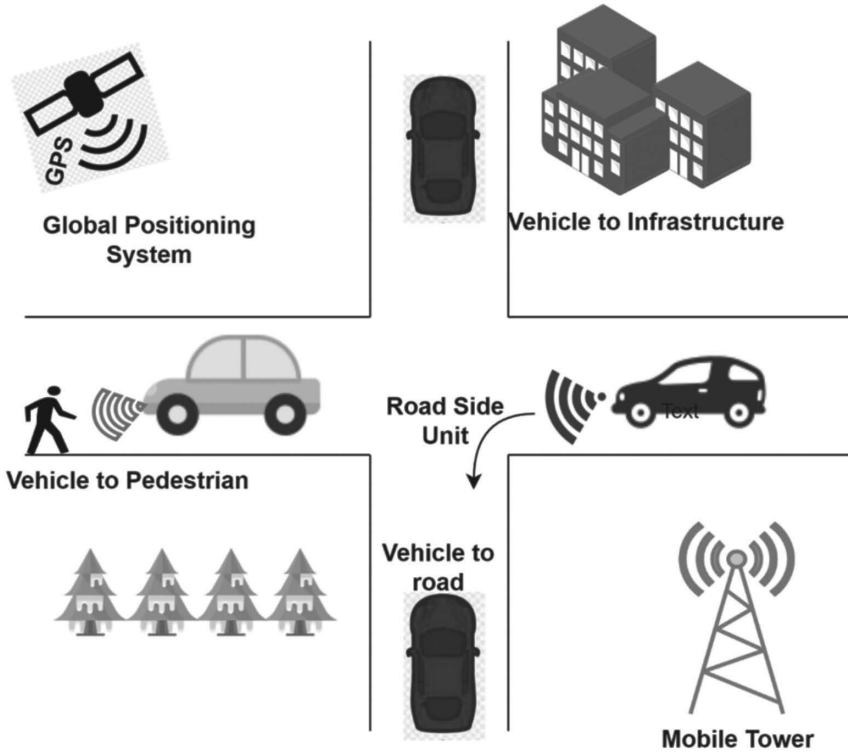


FIGURE 11.1 Modes of communication and connectivity for vehicles, including GPS, vehicle to infrastructure, vehicle to road and building, and vehicle to person.

the ITS industry and has proposed potential solutions for improving the resilience of these systems against cyber threats. Various modes of communication and connectivity for vehicles, including GPS, vehicle to vehicle, vehicle to infrastructure, vehicle to person, and mobile tower, are depicted in Figure 11.1.

11.2 LITERATURE STUDY

To increase the effectiveness and safety of transportation, ITSs depend on related technologies like sensors, communication networks, and cutting-edge data analytics. However, with the increased use of these systems, the risk of cyber attacks against them has also increased. Cyber attacks can have severe consequences, including disruptions to transportation services, loss of revenue, and endangerment of human lives. This literature review examines the different types of cyber attacks against ITSs and the associated impacts. Table 11.1 provides the detail conventional methods employed in cyber attacks targeting ITSs, including their descriptions and constraints.

TABLE 11.1
Standard Techniques Used in Cyber Attacks Against ITS, with Descriptions and Limitations

Reference	Technique Used	Description	Limitations
[25]	Advanced traffic management systems (ATMS)	Intelligent traffic control systems optimize traffic movement and lessen congestion using sensors, cameras, and data analytics.	The associated expenses and intricacy restrict the ability to implement and maintain this. It necessitates reliable network connectivity and proficient data management capabilities.
[26–28]	Vehicle-to-vehicle (V2V) communication	Wireless communication between vehicles to share information about traffic conditions and potential hazards.	The quantity of equipped vehicles and the caliber of wireless communication place restrictions on what is possible. Protocols for strong authentication and encryption are needed.
[29, 30]	Autonomous vehicles	Self-driving vehicles that use sensors and artificial intelligence to navigate roads and traffic.	High expenses and regulatory restrictions impose limitations. To ensure security and dependability, extensive testing and validation are needed.
[31]	Intelligent transportation systems cyber security	Techniques and precautions, such as firewalls, intrusion detection systems, and encryption, safeguard transportation networks from cyber threats.	It is restricted due to the constant need for upkeep and updates and the quick evolution of cyber threats.
[32, 33]	Big data analytics	Techniques and tools are used to analyze large amounts of data from transportation systems to identify patterns, predict traffic flow, and improve system performance.	The lack of advanced data management and analytics capabilities limits the potential. Substantial data gathering and processing are needed.
[34]	Intelligent transportation system simulation	Computer-based models simulate transportation systems and their performance under different scenarios.	The completeness and correctness of the underlying data and assumptions restrict them. Considerable resources and skills are needed to create and sustain.
[35, 36]	Denial of service (DoS) attack	DoS overwhelms a system with traffic or requests, causing it to become unavailable to legitimate users.	Effective against centralized systems but less effective against distributed systems. It can be mitigated with proper network design and monitoring.

(Continued)

TABLE 11.1 (Continued)
Standard Techniques Used in Cyber Attacks Against ITS, with Descriptions and Limitations

Reference	Technique Used	Description	Limitations
[37]	Malware injection	Injecting malicious code into a system, often through a vulnerability in software or firmware.	Effective at gaining access to systems and stealing data but can be challenging to execute against well protected systems. Solid security measures, such as network segmentation and regular patching, can mitigate it.
[38, 39]	Spoofing attacks	Assumes the identity of a genuine user or system to obtain confidential data or take over a system.	Strong security measures, such as multifactor authentication and intrusion monitoring systems, can be used to neutralize this threat. Effective against systems with poor authentication and access restrictions.
[40, 41]	Man-in-the-middle (MITM) attack	Intercepting and altering communication between two systems	Although it can be mitigated by using powerful encryption and authentication methods, it is effective against systems with poor encryption and authentication.
[42, 43]	Physical tampering	Physically manipulating a system, such as by cutting cables or installing unauthorized hardware	Strong physical security measures, like surveillance cams and access controls, can mitigate the effects of this attack in systems with poor physical security.
[44]	Social engineering	Manipulating people to gain access to sensitive information or control over a system, often through deception or persuasion	Effective against those who have not received the appropriate cyber security awareness training, but it can be reduced with ongoing training and awareness efforts

11.3 ITS AND CHALLENGES OF TRANSPORTATION CYBER SECURITY

11.3.1 INTELLIGENT TRANSPORTATION SYSTEMS

A system that uses innovative technology and information processing to increase the effectiveness and security of transit networks is known as an ITS [45]. To provide seamless and sustainable transportation solutions, the ITS seeks to improve

coordination and communication among various modes of transportation, including road, train, air, and sea. Information and communication technologies are applied to ITS to enhance productivity, security, and sustainability. ITS is a broad field encompassing various technologies, including traffic management systems that use real-time data to improve traffic flow, lessen congestion, and increase road safety [46]. To help drivers navigate, park, and prevent collisions, advanced driver assistance systems (ADAS) use sensors and communication technologies [47]. Information and communication technologies are applied to transportation systems as part of the ITS to enhance productivity, security, and sustainability. Communicate with one another and with the road infrastructure using vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication systems, allowing cooperative driving and real-time information exchange [48]. Intelligent public transportation networks that maximize performance using real-time data systems for collecting tolls without making vehicles halt include electronic toll collection (ETC), which uses sensors and communication technologies [49]. Systems with intelligent parking optimize space availability and lessen congestion using sensors and data analytics [50]. Figure 11.2 shows the interaction of vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and infrastructure to infrastructure communication.

11.3.1.1 Examples of ITS Implementation

Adaptive traffic signal management systems can change the timing of traffic signals and enhance traffic flow by using real-time traffic data [51, 52]. On the other hand, adaptive traffic signal management systems use real-time traffic data from numerous sources, including cameras, sensors, or GPS devices, to assess the current traffic conditions. The real-time timing of the traffic signals is then modified using this data to improve traffic movement and ease congestion. For instance, if there is a lot of traffic on one road, the system can change the timing of the traffic signals to give that road more green time while decreasing green time for other roads with less traffic.

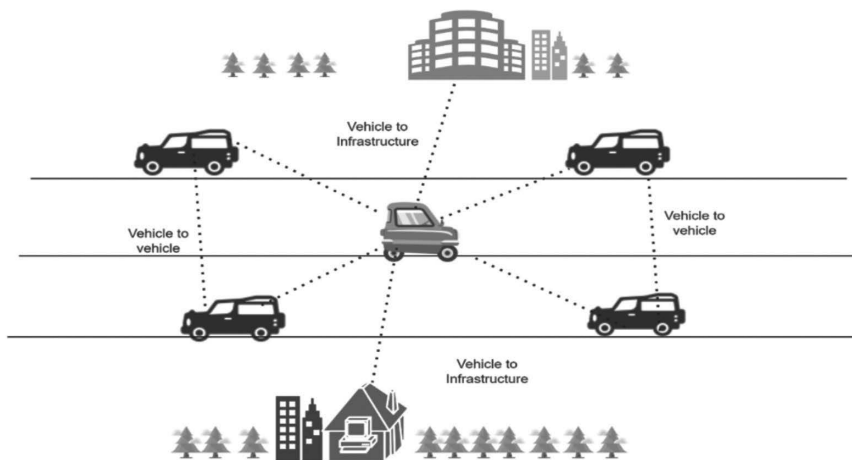


FIGURE 11.2 Vehicle to vehicle (V2V), vehicle to infrastructure (V2I), and infrastructure to infrastructure (I2I) communications.

This may help to ease traffic and shorten commutes for users [53, 54]. Developing connected and autonomous vehicles is a significant technical advancement in transportation. These vehicles have the potential to completely alter the way we move by utilizing cutting-edge sensor, communication, and maritime technologies. The capacity of these cars to increase road safety is one of their most important advantages. With capabilities like automatic emergency braking, collision avoidance, and lane-keeping assistance, they can drastically lower the number of accidents brought on by human error.

Additionally, these vehicles have the potential to reduce traffic congestion and enhance mobility by optimizing traffic flow and reducing the need for parking spaces. As technology advances, the possibilities for connected and autonomous vehicles are endless, and they can potentially transform how we move around our cities and beyond [55]. Improving transportation routes can significantly impact passenger comfort and waiting times. By optimizing routes, public transportation providers can reduce the time passengers spend waiting for their rides and ensure they arrive at their destinations more efficiently. This can be achieved by using GPS tracking and real-time data analysis to predict traffic patterns and adjust routes accordingly. Additionally, improving the physical infrastructure of transportation routes, such as adding sheltered waiting areas and providing accurate information about schedules, can make the experience more comfortable for passengers. Investing in route optimization is crucial in making public transportation more convenient, reliable, and accessible for everyone [56]. Innovative ticketing systems, automatic car location systems, and real-time passenger information systems are examples of the ITS [57].

11.3.2 ITS ECOSYSTEM

The ITS ecosystem refers to the ITS interdependent components, technologies, and stakeholders [58]. The ITS ecosystem includes stakeholders such as government agencies, private companies, research organizations, and end users collaborating to deliver ITS services and solutions. The ITS ecosystem comprises four main elements: infrastructure, vehicles, travelers, and operations. These elements work together to provide a seamless transportation system that is safe, efficient, and environmentally sustainable [6].

11.3.2.1 Infrastructure

ITS infrastructure includes physical infrastructure such as roads, bridges, tunnels, traffic signals, and communication and information systems that enable data flow between infrastructure and vehicles [59]. ITS infrastructure also includes a range of technologies, such as sensors, cameras, and other monitoring devices that capture and analyze data on traffic conditions and road safety. Infrastructure is crucial in developing and deploying ITS. ITS infrastructure refers to the physical and communication systems that support the operation of ITS services, including roads, bridges, tunnels, traffic signals, and other facilities [60].

ITS infrastructure provides a range of benefits, as discussed in the following sections.

- **Data Collection and Analysis:** ITS infrastructure includes various sensors, cameras, and other monitoring devices that capture real-time data on traffic conditions, road safety, and environmental factors [16]. This data is analyzed to provide information on traffic flows, congestion, accidents, and other critical factors that affect the transportation system [61].
- **Communication and Information Systems:** Communication and information sharing among vehicles, infrastructure, and other elements of the transportation system are made possible by the ITS infrastructure. This communication is essential for providing passengers with real-time traffic updates, alerts, and notifications, as well as for enhancing safety and easing congestion [62, 63].
- **Intelligent Traffic Management:** ITS infrastructure includes advanced traffic management systems that use real-time data and predictive analytics to manage traffic flows, optimize traffic signals, and reduce congestion. This system ensures that the transportation network operates efficiently, reducing travel times and improving safety [64].
- **Sustainable Transport Solutions:** ITS infrastructure enables the integration of sustainable transport modes such as cycling, walking, and public transportation. This integration is crucial for easing traffic, enhancing air quality, and encouraging more environmentally friendly journey habits. The development and deployment of the ITS infrastructure require collaboration among various stakeholders, including government agencies, private companies, and research organizations. ITS infrastructure must be designed to be integrated, interoperable, and scalable to support future developments in ITS technology [64].

11.3.2.2 Vehicles

The ITS ecosystem depends heavily on vehicles because they provide a means of transportation and are outfitted with various technologies that allow them to interact with other vehicles and the infrastructure [65]. The goal of ITS vehicles is to offer safer, more effective, and ecologically friendly transportation. Vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication, GPS, collision avoidance systems, and other safety features are just a few of the technologies that are included in ITS cars. Through the use of these technologies, ITS vehicles can interact with other vehicles and infrastructure, giving real-time data on traffic patterns, road safety, and environmental factors [66]. Vehicles can interact with one another via a V2V network, sharing data on location, speed, and other aspects of driving. This information can be used to enable collision avoidance systems and improve safety. V2I communication enables vehicles to communicate with infrastructure, providing real-time information on traffic signals, road signs, and other infrastructure, enabling real-time traffic management and control systems that optimize traffic flows, reduce congestion, and improve safety [67]. ITS vehicles can also be designed to support alternative modes of transportation, such as cycling, walking, and public transport [68]. For example, ITS vehicles can provide real-time information on public transportation schedules, routes, and availability, encouraging travelers to use public transportation instead of driving.

In addition, ITS vehicles can be designed to be more environmentally sustainable, reducing emissions and promoting sustainable transportation. For example, ITS vehicles can be equipped with hybrid or electric powertrains, reducing emissions and promoting sustainable transportation. The development and deployment of ITS vehicles require collaboration among various stakeholders, including vehicle manufacturers, government agencies, private companies, and research organizations. Integrating ITS vehicles into the transportation system can help reduce travel times, improve safety, and enhance the overall efficiency of the transportation system [66].

11.3.2.3 Travelers

Travelers are crucial in the ITS ecosystem. ITS is a system of related technologies and infrastructure that improves transportation efficiency, safety, and environmental sustainability. Travelers interact with these technologies and techniques in various ways, and their behavior and feedback can impact the effectiveness of the ITS ecosystem [69].

Here are some specific ways in which travelers contribute to the ITS ecosystem.

- **Using ITS Technologies:** Travelers use various ITS technologies such as navigation apps, traffic information systems, public transportation apps, and smart parking systems. Using these technologies, travelers can make informed decisions about their travel plans, avoid traffic congestion, and reduce their carbon footprint [69].
 - **Providing Feedback:** Travelers can provide feedback to ITS operators and transportation agencies through various channels, such as social media, surveys, and customer service hotlines. This feedback can help improve the performance of ITS systems and inform future development [69].
 - **Adapting to New Technologies:** As ITS technologies evolve, travelers must adapt to new systems and interfaces. This adaptation can be challenging, but it is essential to ensure that travelers can use these technologies effectively [69].
- Following Rules and Regulations:** ITSs rely on the cooperation of travelers to function effectively. This includes following traffic laws, obeying public transportation rules, and respecting the safety and privacy of other travelers [69].

11.3.2.4 Operations

ITS operations play a critical role in the ITS ecosystem by managing and coordinating the various technologies and infrastructure that comprise the system. ITS operations involve planning, designing, implementing, and maintaining transportation technologies, including traffic management, transit, and traveler information systems. Here are some specific ways in which ITS operations contribute to the ITS ecosystem [70]:

- **System Monitoring and Management:** ITS operations personnel monitor transportation systems and traffic flow in real time, identifying issues and taking corrective actions to minimize disruptions to traffic flow and safety [70].

- **Incident Response:** ITS operations personnel respond to incidents such as accidents, roadway obstructions, and weather-related events, providing timely information to travelers and coordinating with emergency services to ensure incidents are cleared safely and efficiently [70].
- **Data Collection and Analysis:** ITS operations collect and analyze transportation data, including traffic volume, travel time, and weather conditions, to identify trends and patterns and to inform future planning and decision making [71].
- **System Optimization:** ITS operations personnel optimize transportation systems by implementing traffic signal coordination, ramp metering, and variable message signs to reduce congestion, improve safety, and enhance travel time reliability [70].
- **Interagency Coordination:** ITS operations personnel work closely with other transportation agencies, including public transportation providers and emergency services, to coordinate responses and improve overall transportation efficiency and safety [70].

11.3.3 SECURING THE ITS ECOSYSTEM

Securing the ITS ecosystem is crucial to ensure critical transportation infrastructure's safe and reliable operation. Here are some key measures that can be taken to secure the ITS ecosystem [72]:

- **Implement Access Control:** Access control is essential to guarantee that only authorized employees can access the ITS ecosystem. Strong authentication and authorization mechanisms, such as role-based access control and multifactor authentication, can be implemented to accomplish this [73].
- **Use Encryption:** Encryption can help to secure data in transit and at rest. Implementing encryption for data transmission and storage can prevent unauthorized access to sensitive information [72].
- **Regularly Update Software:** Regular software updates can help to mitigate vulnerabilities in the ITS ecosystem. Organizations should ensure that software updates are regularly applied to all ITS ecosystem components [72].
- **Implement Firewalls and Intrusion Detection Systems:** Unauthorized entry to the ITS ecosystem can be found and prevented with firewalls and intrusion detection systems. By monitoring network traffic and identifying potential security threats, these systems can help to protect the ITS ecosystem from cyber attacks.
- **Conduct Regular Security Assessments:** Weaknesses in the ITS system can be found with the help of routine security audits. Organizations should routinely conduct vulnerability assessments and penetration testing to find possible security weaknesses and take corrective action [72].
- **Educate Employees:** Employees are often the weakest link in the security chain. Educating employees on cyber security best practices and the importance of security can help to reduce the risk of cyber attacks [72].

- **Develop an Incident Response Plan:** Organizations can react to security incidents more quickly and successfully with an incident response plan. Organizations should have a well-defined incident response plan with clear communication and escalation procedures [72].

11.3.4 ANTI-PHISHING SOLUTIONS

Phishing attacks are a significant concern in securing the ITS ecosystem. Various anti-phishing solutions can be implemented to enhance the security of ITS against phishing attacks. Here are some of the most effective anti-phishing solutions[74]:

- **Email Filters:** Before phishing emails arrive in a user's inbox, email filters are an efficient way to identify and stop them. They use block lists, allow lists, and content analysis to identify suspicious emails and prevent them from being delivered [74].
- **Web Filters:** Web filters can block access to known phishing websites and prevent users from accidentally visiting them [75]. They can analyze web content for suspicious activity or use URL filtering to block known phishing domains.
- **Multifactor Authentication (MFA):** MFA is an additional layer of security that requires users to provide further information, such as a code sent to their mobile device. It helps prevent phishing attacks that rely on stolen login credentials [74].
- **Security Awareness Training:** To stop phishing assaults, security awareness training is essential. It teaches users how to recognize and avoid phishing emails, verify the authenticity of websites, and report suspicious activity [74].
- **DNS Filtering:** DNS filtering is another effective way to block access to known phishing domains and prevent users from accessing them. It uses DNS block lists or reputation-based filtering to protect against phishing attacks [74].
- **Anti-Malware Solutions:** Malware that might have been installed due to a phishing attack can be found and removed using anti-malware tools. To defend against various threats, they combine signature-based and behavior-based analysis [74].
- **Breach Detection Systems (BDS):** ITSs are intricate systems that combine numerous technologies to increase movement, safety, and effectiveness in transportation [76]. Because of their growing importance, ITSs have turned into a top target for cyber attacks. Breach detection systems (BDSs) are essential for protecting the ITS environment. To identify and notify security employees of possible security breaches, breach detection systems watch network traffic, system records, and other security-related data. A BDS employs various strategies to find potential security threats in the ITS environment, including signature-based, behavior-based, and anomaly-based detection methods [77]. Signature-based detection uses known attack patterns to detect possible security breaches. Behavior-based detection

monitors system behavior for abnormal activities that may indicate a security breach. Anomaly-based detection detects abnormal patterns that may indicate a security breach. The benefits of implementing a breach detection system in an ITS ecosystem are:

- **Early Detection of Security Threats:** The BDS detects potential security breaches early, reducing the time needed to investigate and respond to the threat [78].
 - **Mitigation of Security Risks:** By detecting potential security breaches early, a BDS can mitigate the cyber attack risk and prevent possible damage.
 - **Compliance with Regulations:** Implementing a BDS can help organizations comply with security and data privacy regulations.
 - **Improved System Performance:** By monitoring system behavior, a BDS can identify and address issues affecting system performance before they cause significant disruptions.
- **IPS/IDS:** Two critical elements in the ITS ecosystem's security are the IPS (intrusion prevention system) and IDS (intrusion detection system) [79]. An IDS security instrument monitors network data to spot and warn managers of potentially harmful or suspicious behavior. It examines and contrasts network data with a library of recognized attack fingerprints or patterns. The IDS alerts the supervisor or security staff when an attack is found. On the other hand, an IPS detects attacks and takes action to prevent them. It uses the same techniques as an IDS to analyze network traffic, but, when it identifies an attack, it can block or quarantine the malicious traffic to prevent it from reaching its target. In the context of ITS, an IDS or IPS can help protect critical systems and data from cyber threats. These threats can come from various sources, including hackers, malware, and other malicious actors. By monitoring network traffic and blocking suspicious activity, an IDS or IPS can help prevent attacks that could disrupt or compromise the functioning of the transportation system [80].

However, it's important to note that an IDS or IPS is just one part of a comprehensive security strategy for ITS. Other measures, such as encryption, access controls, and security audits, should also be implemented to ensure the security and reliability of the system. Additionally, regular updates and maintenance of the IDS or IPS are essential to keep up with evolving threats and ensure the continued effectiveness of security measures [81].

11.3.5 CHALLENGES OF TRANSPORTATION CYBER SECURITY

Cyber security in the transportation industry faces several difficulties in defending against online attacks. We will examine some of these challenges in this section [82].

- **Complexity of Transportation Systems:** Transportation systems are complex, with multiple systems and subsystems working together to ensure safe

and efficient transportation [83]. This complexity makes it challenging to identify vulnerabilities and secure the system against cyber threats. For example, a transportation system may comprise multiple software systems, hardware devices, and networks, each with different levels of security and vulnerabilities.

- **Cost of Cyber Security:** Cyber security measures can be costly, and transportation companies may face budgetary constraints that make it challenging to allocate resources to cyber security [84]. Additionally, cyber security requires ongoing maintenance and updates, which can further increase the cost of implementation.
- **Legacy Systems:** Transportation systems often rely on legacy systems that may not be compatible with modern cyber security measures [85]. These legacy systems may be challenging to update or replace, making them vulnerable to cyber threats [86]. For example, an old control system in a train may not be compatible with modern cyber security measures, making it easier for cyber attackers to exploit vulnerabilities.
- **Insider Threats:** Insider threats pose a significant challenge to transportation cyber security. Employees, contractors, and other insiders may have access to critical systems and data, making them potential threats to the system's security [87].

11.4 CYBER SECURITY IN TRANSPORTATION SYSTEMS AND VULNERABILITIES IN TRANSPORTATION SYSTEMS

11.4.1 CYBER SECURITY IN INTELLIGENT TRANSPORTATION SYSTEMS

The result of the fusion of several technologies, including wireless networks, control systems, real-time data, embedded systems, and machine learning, is the Internet of Things (IoT) [88]. The Internet of Things (IoT) includes products that relate to concepts like the intelligent home, intelligent healthcare system, intelligent community, etc., from the consumer's viewpoint. These areas have many characteristics and problems in common. It is usual for IoT subfields to share technology, but this practice needs to be carefully considered and investigated. Despite their similarities, different industries have different requirements for transmission range and bit rate, real-time operation, dependability, and security. Several IoT characteristics define ITS for smart cities. They can be recognized by their rigid deadlines, dynamic character, and enormous datasets. The crucial requirement for safety is one of the key characteristics that distinguish the ITS. ITS applications lie under the following three categories: efficient road traffic, entertainment, and transportation safety [89, 90]. Apps enhancing road safety must meet high cyber security requirements and adhere to rigorous real-time deadlines. Cyber security standards are pretty strict because even while the effectiveness of infotainment applications and traffic flow efficiency isn't directly tied to the physical safety of road users, a security breach in any of them might endanger the effectiveness of the entire ITS [71].

11.4.2 CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS

Cyber security attacks on transportation systems refer to the deliberate exploitation of vulnerabilities in information technology infrastructure used in transportation systems. These attacks can disrupt the normal functioning of transportation systems, cause damage to critical infrastructure, and even result in the loss of human lives [91]. These attacks can take many forms, including malware and viruses that infect transportation systems' networks, servers, or end user devices and cause disruptions or data loss; denial of service attacks that overload or flood transportation systems' networks with traffic, causing them to crash or become unavailable [92]; social engineering attacks that exploit human vulnerabilities through phishing, pretexting, or baiting to trick users into divulging sensitive information or installing malware[44]; ransomware attacks that encrypt critical data and demand payment for decryption [93]; long-term, targeted attacks against transportation systems that are used by advanced persistent threats to access confidential data, such as financial transactions, private information, or logistics plans, without authorization.

11.4.3 IMPORTANCE OF TRANSPORTATION SYSTEMS TO SOCIETY AND THE ECONOMY

Cyber security attacks on transportation systems can have severe consequences, including flight cancellations, delays, or disruptions to shipping and supply chain operations, risking passenger safety and causing significant economic losses. Therefore, protecting transportation systems against cyber attacks is crucial to ensure their uninterrupted functions and safeguard public security [94]. Transportation systems play a critical role in society and the economy by facilitating the movement of people, goods, and services from one location to another. Here are some of the crucial reasons why transportation is essential:

- **Facilitating Economic Activity:** Transportation systems are essential for moving goods and services that drive economic activity. Businesses require efficient transportation to transport their products to customers, obtain raw materials and supplies, and carry their employees to and from work [94].
- **Supporting Employment:** Transportation systems support jobs across various sectors, including trucking, shipping, air travel, and public transportation. These jobs provide livelihoods for millions of people worldwide [94].
- **Enabling Access to Goods and Services:** Transportation systems give individuals access to essential goods and services, including food, medicine, and other necessities. This is particularly important for people who live in remote areas where these goods and services are not readily available [94].
- **Enhancing Social Mobility:** Transportation systems can help people access education, healthcare, and employment opportunities they might not otherwise have access to. This is particularly important for disadvantaged groups who may face barriers to mobility [94].

- **Promoting Tourism:** Transportation systems are critical for the tourism industry, enabling people to visit different parts of the world and explore new cultures [94].

11.4.4 VULNERABILITIES IN TRANSPORTATION SYSTEMS

Transportation systems are vulnerable to various risks and vulnerabilities, which can significantly impact people's safety, economic activities, and the environment [95]. Some of the most common vulnerabilities in transportation systems include:

- **Cyber Security Vulnerabilities:** Transportation systems rely heavily on computerized systems, which can be vulnerable to cyber attacks. For example, a cyber attack on a transportation system's control system can cause significant disruptions, including the shutdown of critical infrastructure such as airports, railways, and ports [96].
- **Infrastructure Vulnerabilities:** Transportation infrastructure, such as bridges, tunnels, and highways, can be vulnerable to natural disasters like floods, earthquakes, and hurricanes, as well as human-made disasters like terrorism and sabotage [97].
- **Human Error:** Transportation systems can be vulnerable to human error, such as a train driver falling asleep, a pilot making a navigation error, or a truck driver losing control of the vehicle [98].
- **Operational Vulnerabilities:** Transportation systems can also be vulnerable to operational failures, such as mechanical or technical failures, inadequate maintenance, or insufficient personnel training [99].
- **Physical Security Vulnerabilities:** Transportation systems can be vulnerable to physical security threats such as terrorism, hijacking, and criminal activities like theft and vandalism [95].
- **Environmental Vulnerabilities:** Environmental risks such as air pollution, greenhouse gas emissions, noise pollution, and the effects of climate change can make transportation networks vulnerable. Transportation systems must implement robust security and risk management techniques to reduce these vulnerabilities. In addition to powerful regulatory frameworks and emergency reaction plans, these measures could include cutting-edge technologies like sensors, monitoring systems, and predictive analytics. Additionally, public education and awareness initiatives can assist people in better comprehending the dangers and weaknesses connected to transportation systems and taking the necessary precautions to lessen them [95].

11.5 TYPES OF CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS/ITS ATTACK VECTORS

Infrastructures that facilitate the movement of people, goods, and services across the globe include transportation systems. They play a crucial role in contemporary culture and rely heavily on technology. Sadly, their reliance on technology also

exposes them to various cyber security assaults. A computer system called an ITS or Industrial Control System manages and controls industrial operations. Critical infrastructure industries like electricity, water, transportation, and manufacturing frequently use these systems. Serious repercussions from an attack on an ITS can include service interruption, property harm, and even fatalities [100, 101].

The following sections include some of the typical attack methods that can be employed when targeting an ITS.

11.5.1 PHISHING ATTACKS

One of the most frequent cyber security attacks that can happen in any business is phishing [102]. These attacks trick workers into disclosing private information or downloading malware in the transportation industry. An employee might, for instance, get an email asking for details on a shipment or a customer that appears to be from a reliable source, like a shipping business. The employee may be required to input their login information when the email contains a link to a fake website that mimics the real one. Once the attacker has the login information, they can view private data and even take over the transportation network [103, 104].

11.5.2 RANSOMWARE ATTACKS

Another kind of cyber attack that can be devastating to transportation networks is ransomware. These attacks involve gaining access to a system, where the attacker encrypts all the data and renders it useless until a ransom is made. This could cause a total shutdown of the transportation system, causing delays and financial losses. Attackers have occasionally threatened to divulge private information if the ransom is not paid, which could harm the image and security of the transportation system [105].

11.5.3 DDoS ATTACKS

A distributed denial of service (DDoS) attack is an assault that includes saturating a system with traffic to overwhelm its servers and bring them down. This could cause the transportation system to close entirely, causing delays and financial losses. Attackers can also use DDoS attacks to divert security employees and conduct additional attacks, like data theft or malware installation [106]. Figure 11.3 depicts that the perpetrator initiating a DDoS assault on the website of the target by inundating the DNS service with malevolent traffic.

11.5.4 SOCIAL ENGINEERING ATTACKS

Attacks using social engineering persuade people to reveal sensitive information or take action. Attackers may adopt employee, vendor, or customer personas to obtain sensitive data. They might also use phony documents or websites to win the victim's confidence. These assaults may be challenging to identify and cause sizable financial damages or data breaches [107].

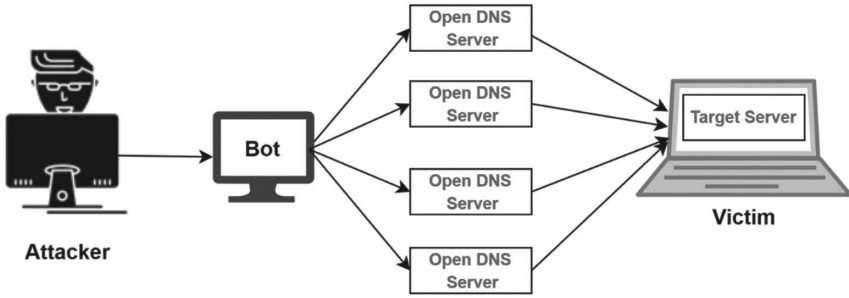


FIGURE 11.3 Attacker launches a DDoS attack on a victim’s website by overwhelming the DNS service with malicious traffic.

11.5.5 INSIDER ATTACKS

Attacks carried out by employees or other authorized people are called insider attacks. These assaults, which may or may not be deliberate, can cause system crashes, data leaks, and other harm. Insiders may have access to sensitive data or networks, and they may take advantage of this access for their benefit or to launch an attack on behalf of an external attacker [108].

11.5.6 PHYSICAL ATTACKS

Attackers physically gain entry to the ITS and modify its hardware or software. Physical assaults can involve anything from taking login information to destroying the system [109]. Cyber security attacks of all kinds can affect transportation networks [110]. The attacks, as mentioned earlier, are just a few instances of the different types that can occur. To defend against these dangers, transportation systems need to be put in place robust cyber security measures like firewalls, intrusion detection systems, and access limits. Employers must regularly educate their staff on cyber security best practices to stop these attacks. Physical attacks on ITS involve gaining physical access to the system and tampering with its hardware or software components. Here are some examples of physical attacks on ITS [111].

- **Tampering with Equipment:** Attackers can physically tamper with the equipment in an industrial facility to cause damage or disrupt operations. For example, they may manipulate valves or switches to cause industrial processes to malfunction or damage equipment [111].
- **Theft of Equipment:** Attackers may steal equipment like laptops or USB drives to control the ITS. They can then use the stolen equipment to gain unauthorized access to the system or steal sensitive data [111].
- **Sabotage:** Sabotage involves intentionally causing damage or disruption to the ITS. For example, an attacker could cut power or communication cables, damage control systems, or introduce malicious software to disrupt industrial processes [112].

- **Social Engineering:** Social engineering attacks involve manipulating people to gain access to the ITS. For example, an attacker may pose as a technician or vendor and gain access to the facility to install malware or steal sensitive information [112].
- **Physical Intrusion:** Attackers can physically intrude into a facility to gain access to the ITS. This could involve bypassing security controls or exploiting vulnerabilities in physical security systems [108]. To protect against physical attacks on an ITS, it is essential to implement physical solid security controls, such as access controls, surveillance systems, and intrusion detection systems. Regular security assessments and training of employees on cyber security best practices can also help to mitigate the risk of physical attacks on ITS. Additionally, organizations should have an incident response plan to respond quickly and effectively during a physical attack [111].

11.6 CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS: IMPACT AND PREVENTION

11.6.1 IMPACT OF CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS

- **Economic Impact:** Cyber security attacks can have a significant economic impact on transportation systems. For example, a successful attack on a transportation system could result in substantial financial losses due to the disruption of operations, decreased productivity, and increased expenses associated with incident response and recovery [113, 114].
- **Public Safety Impact:** Cyber security attacks on transportation systems can also significantly impact public safety. If attackers can gain control of critical systems such as traffic lights, railway signals, or airport control towers, it could lead to accidents, injuries, and even loss of life [113].
- **Reputation Impact:** A successful cyber attack on a transportation system can damage the reputation of the affected company or organization. Customers and the general public may lose confidence in the organization's ability to provide a safe and reliable service [113].
- **Psychological Impact:** Cyber security attacks can also have a psychological impact on the public. Suppose a successful attack on a transportation system leads to injuries or loss of life. In that case, it can have a significant emotional impact on those affected and on the broader community [113].

11.6.2 PREVENTING CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS

Cyber security attacks on transportation systems can have severe consequences, from disrupting services to ending human lives. Here are some strategies that can help prevent such attacks [115].

- **Best Practices for Cyber Security in Transportation Systems:** Organizations operating transportation systems should follow best practices

for cyber security, such as implementing strong password policies, regular system updates, and multifactor authentication [116].

- **Developing a Cyber Security Culture:** Developing a culture of cyber security awareness among employees and stakeholders can help prevent cyber security attacks. This includes regular training and education on and avoiding cyber security risks [116].
- **Risk Management Strategies:** Risk management strategies can help organizations identify and mitigate cyber security risks. This includes conducting regular risk assessments and implementing security controls to reduce the impact of threats [116].
- **Incident Response Planning:** Organizations should have an incident response strategy in place to react to cyber security problems swiftly and efficiently. The steps in this strategy should cover incident detection, reporting, and response [116].
- **Coordinated Efforts Among Government, Industry, and Academia:** Collaboration among the public sector, private sector, and academic institutions can aid in preventing cyber attacks on transportation networks. Information and resources are shared to recognize and reduce cyber security threats [2].

11.7 ITS ATTACKER MOTIVES

Find the reason that certain ITS attackers have for digging in deeper on certain things your company might hold in store for them [117]. Knowing the right reasons might make your organization technically strong enough to defend against those attacks as well. When ITS attackers hijack systems, their intentions can be identified according to the type of data they steal. You may fortify your defenses and be ready for anything the threat landscape throws your way if you can more clearly understand why hackers hack (their motivations) and who will most likely target your particular company. (It should be emphasized that because the word “crime” is a legal term and an attack may or may not be regarded as one, it is not used here. As a result, the term “attack” is utilized.) There are typically six reasons for trying to launch a cyber attack, according to Mark Heptad [118], which are discussed in the following sections. Figure 11.4 depicts a scenario in which an individual with malicious intent sends a message that results in the unauthorized access of confidential files. This individual is strongly driven to carry out his actions.

11.7.1 FINANCIAL SUCCESS

Hackers are primarily motivated by money, and there are numerous methods to acquire it [119]. They might hack your financial websites’ passwords, gain access to your bank or investment accounts directly, and then move money to one of their accounts. Or they could attack your entire business with malware. They can also use a complex spear phishing scam to trick an employee into sending money [120]. Despite the abundance of choices, most hackers seek to make money. A well-known illustration of the financial motivation behind cyber attacks is the theft of personally

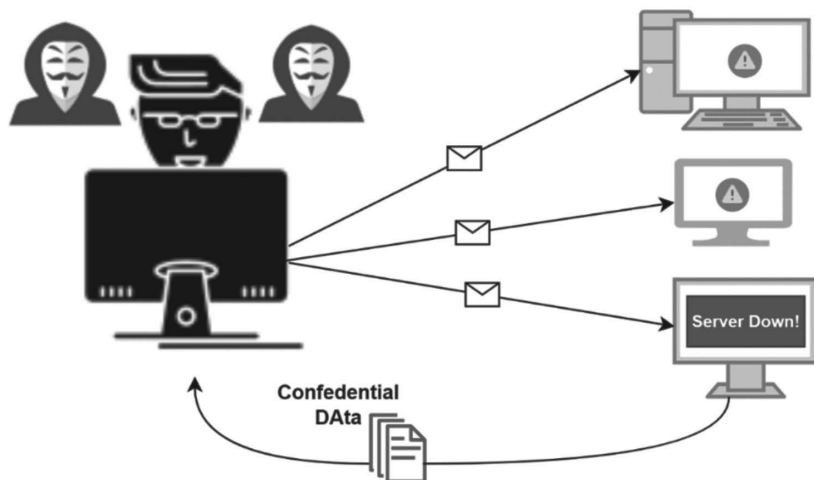


FIGURE 11.4 Hacker sends a malicious message and gains access to confidential files.

identifiable information (PII), which is then sold. This motive accounts for many cyber attacks against retailers and healthcare facilities, typically carried out by organized criminal gangs. A well-known illustration of the financial motivation behind cyber attacks is the theft of personally identifiable information (PII), which is then sold. This motive accounts for many cyber attacks against retailers and healthcare facilities, typically carried out by organized criminal gangs [121].

11.7.2 APPRECIATION AND SUCCESS

Some hackers are motivated by the feeling of accomplishment from breaking into an extensive system. Everyone desires to be noticed, whether they work alone or with others in groups. This is connected to the notion that cyber criminals are challenging, competitive individuals who enjoy the task that their actions present. Even now, they frequently motivate one another to perform more difficult attacks [122].

11.7.3 INTERNAL THREATS

People with access to crucial information or systems may abuse it, which would be bad for their firm. These dangers are among the biggest threats to a company’s cyber security because they could come from partners, vendors, contractors, or internal workers. Yet not all insider risks are intentional, according to a Crowd Research Partners report. The majority (51%) are the consequence of negligence, carelessness, or fabricated credentials. However, harm might still happen even in unforeseen circumstances [123]. Many different kinds of data, such as economic data, data on sales, customer details, shipping data, automobile tracking data, intellectual property, business operations data, personally identifiable information (PII), proprietary data, and other types of data, are susceptible to theft and monetization. The stolen

data can be used to perpetrate crimes and threats linked to information theft, including identity theft, privacy breaches, financial fraud, industrial espionage, and more [124]. Nation and dishonest competitors are two of the most common data thieves. Their objectives range from acquiring a competitive edge, particularly in contract bidding, to replicating pricey studies, spotting operational flaws, enhancing corporate procedures, etc. [123].

11.7.4 INFORMATION WARFARE AND “HACKTIVISM” WITH A POLITICAL MOTIVATION

Using their expertise in hacking, specific cyber criminal organizations go after giant firms. They are often motivated by a cause, such as bringing attention to human rights issues or alerting a significant company to system flaws. They might also come up against groups whose viewpoints conflict with their own. These organizations may claim they are exercising their right to free expression when they steal data. Still, they almost always use DDoS (distributed denial of service) attacks to saturate a website with traffic and bring it to a halt. The relevant educational episodes are (listed in section 11.7.5) [125]. They launch a distributed denial-of-service attack (DDoS) against the ITS infrastructure to take down the systems and cause chaos on the roads [126] and use company apps or websites to post political, critical, or prank remarks. Another goal is to harm the reputation of the ITS firm and cause financial damage for it [127]. Hacking roadside dynamic message signs to display satirical, political, or other messages is another goal [128]. When cooperative autonomous vehicles are a reality on public roads, thieves could be able to send phony V2V messages to disrupt traffic. In the future, dishonest companies might pay criminals to taint V2V channels with V2V information poisoning, so that autonomous vehicles pass by their destinations [129].

11.7.5 THEFT IN VEHICLES AND SYSTEMS

The theft of commodities or valuables within vehicles, or even the vehicles themselves, would be one of the most alluring profit-making models for criminals. Certain people can try to take advantage of ITS systems to avoid paying service fees. A number of assaults have been found [130]:

- Hacking autonomous trucks and rerouting them to a remote place (like a deserted parking lot outside of a town) so that thieves can break in and take the cargo.
- Covertly using compromised autonomous vehicles to convey illegal goods like drugs and weapons.
- Hacking driverless cars to give them instructions to reroute to a secret place, where thieves can take goods from the passengers or possibly kidnap the passengers.
- Delivering and stopping autonomous vehicles to steal them or their parts.
- Using compromised ITS systems to get out of paying fees for services like parking, bridge tolls, congestion charges, etc.

Computer-controlled traffic lights with integrated preemption receivers can be remotely changed using mobile infrared transmitter (MIRT) devices:

- Future technologies could include sophisticated MIRT-style devices that can alter traffic patterns in the owner's favor.
- Untrustworthy ITS service providers (such as autonomous taxi and delivery service providers) can try to stifle competition by hacking the autonomous vehicles of their rivals and disabling them.
- An autonomous vehicle on a dedicated road can be illegally given a higher priority so that other autonomous cars can pass.
- Rideshare orders for autonomous vehicles can be faked to bill unwary customers [131, 132].

11.7.6 REVENGE AND NUISANCE

The majority of cyber attacks motivated by retaliation are often carried out by disgruntled current or former workers [133]. Disgruntled ex-employees attacking their ex-employers are a frequent occurrence in the news. Some people have no other motivation than to attack a person or an organization to cause chaos and destruction. Unfortunately, such is the case. The renowned bank robber “slick” Willy Sutton, the bank robber, is a prime example. According to reports, when questioned, he claimed he robbed banks because “that is where the money is.” He said that he “just enjoyed robbing banks.” Money wasn’t a driving force [134].

11.8 CASE STUDIES OF CYBER SECURITY ATTACKS ON TRANSPORTATION SYSTEMS

11.8.1 UKRAINE POWER GRID ATTACK (2015)

One of the most well-known cyber security assaults on a transportation system occurred in 2015 when the power grid in Ukraine was attacked. In the attacks of December 2015, malware called Crash Override specifically targeted the Ukrainian power infrastructure [135]. Three power distribution firms in Ukraine had their control systems breached by hackers in December 2015. The attackers were able to seize control of the electrical grid and turn off the electricity for more than 225,000 consumers. It was the first time a cyber attack on a power infrastructure was known to cause a widespread blackout. The attackers employed various strategies to access the management systems, including spear-phishing emails, malware, and remote access tools. Once they gained entry, they could take over the systems and send orders to turn off the electricity. Although the Russian government denied any participation, it was thought that a group of Russian hackers were responsible for the assault. The assault had a significant negative economic and social effect because it left homes and businesses without electricity during the winter. Additionally, it sparked worries about how susceptible vital infrastructure is to cyber attacks and the possibility that other nations could experience similar attacks.

Since the attack, there has been increased attention on critical infrastructure security and efforts to improve cyber security in the transportation sector. This attack serves as a reminder of the value of solid cyber security measures and the necessity for enterprises to take preventative actions to safeguard their systems from online dangers. It also highlights the potential consequences of cyber attacks on transportation systems and the need for coordinated responses to mitigate their impact [135, 136].

11.8.2 ATLANTA TRANSPORTATION SYSTEM RANSOMWARE ATTACK (2018)

The city initially refused to pay the ransom and instead worked to restore its systems and files. However, the attack still had significant economic and social impacts, with the disruption to transportation services causing delays and frustration for residents and businesses [137]. The attackers, in this case, have not been publicly identified. Still, the incident highlighted the growing threat of ransomware attacks on transportation systems and the need for robust cyber security measures to prevent and respond to these threats. Following the attack, the city of Atlanta invested in significant upgrades to its cyber security infrastructure and implemented new policies and procedures to improve its overall cyber security posture [138].

11.8.3 NOTPETYA MALWARE ATTACK ON SHIPPING COMPANY MAERSK (2017)

Another special cyber security attack on a transportation system happened in 2017 when the NotPetya malware was directed at the shipping company Maersk. In June 2017, malware called NotPetya was released, targeting computer systems worldwide. One of the companies affected was Maersk, one of the world's largest shipping companies. The malware quickly spread through Maersk's computer systems, encrypting data and disrupting operations. The attack significantly impacted Maersk's operations, with many of the company's systems and processes being disrupted or shut down. This included the company's email system, its customer-facing booking systems, and its container tracking systems. The disruption to Maersk's operations had a significant economic impact, with the company estimating losses of up to \$300 million as a result of the attack [135].

The attackers behind the NotPetya malware have not been publicly identified, but it is believed to have originated in Russia and to have been targeted at Ukrainian infrastructure. However, the malware's fast spread meant that it affected many companies worldwide, including Maersk. The attack highlighted the potential vulnerability of transportation systems to cyber attacks and the need for robust cyber security measures to prevent and respond to these threats. It also highlighted the potential economic impact of cyber attacks on transportation systems and the need for coordinated responses to mitigate their impact. In the aftermath of the attack, Maersk invested heavily in upgrading its cyber security infrastructure and implemented new policies and procedures to improve its overall cyber security posture [139, 140].

11.8.4 WANNACRY RANSOMWARE ATTACK ON UK'S NATIONAL HEALTH SERVICE (2017)

The 2017 NHS (National Health Service) WannaCry ransomware attack had a significant effect on logistics and transportation services even though it wasn't specifically a transportation system [133]. The following happened: The WannaCry ransomware assault infected over 200,000 computers worldwide in May 2017, including NHS computers. The attack encrypted the data on the impacted computers, and a ransom demand was made in exchange for the decryption key. The attack caused significant disruption to or shut down numerous NHS computer systems, including those used for patient data and appointment scheduling. This led to the cancellation of thousands of appointments and surgeries, and some patients were diverted to other hospitals. The attack also affected the transportation of medical supplies and equipment, with some deliveries delayed due to disruptions to logistics systems.

Although the perpetrators of the WannaCry ransomware attack have not been publicly named, North Korea is thought to be the attack's country of origin. The attack highlighted the possible repercussions of cyber attacks on vital infrastructure and the requirement for effective cyber security means to address and stop these threats. It also highlighted the interconnectedness of transportation systems with other critical infrastructures and the potential impact of attacks on transportation-related logistics and supply chains. Following the attack, the NHS invested heavily in upgrading its cyber security infrastructure and implemented new policies and procedures to improve its overall cyber security posture. The attack also increased cyber security attention in other critical infrastructure sectors, including transportation [141, 142].

11.8.5 STUXNET ATTACK ON IRANIAN NUCLEAR FACILITIES (2010)

In 2010, researchers discovered Stuxnet, a type of malware developed mainly to target ICSs used in nuclear power plants [143]. The virus, intended to attack Iran's centrifuges used to enrich uranium, was thought to have been developed by the U.S. and Israeli governments. The attack had potential impacts on transportation systems because disruption to Iran's nuclear program could have led to political and economic instability in the region, potentially affecting the transportation of goods and resources. In addition, the use of cyber attacks as a tool of statecraft highlighted the potential risks of cyber warfare and the need for robust cyber security measures to prevent and respond to these threats. The Stuxnet attack was notable for its sophistication and for being one of the first known examples of a cyber weapon used in a state-sponsored attack. It highlighted the growing importance of cyber security in national security and led to increased attention on the potential impacts of cyber attacks on critical infrastructure, including transportation systems. Since the Stuxnet attack, there have been many other examples of cyber attacks on critical infrastructure, including transportation systems. Governments and private sector organizations have invested heavily in upgrading their cyber security infrastructure to prevent and respond to these threats [144, 145].

11.9 COLLABORATIVE APPROACHES TO INTELLIGENT SECURITY IN IOT

A clever and proactive protection approach is necessary, given the complexity of ITS. The methods covered in this section pertain to the all-encompassing strategy for ITS cyber security and have been successfully applied in security systems in several fields. There aren't many experimental results of their use in ITSs, even though they are frequently mentioned as strategies that will influence the ITS's overall appearance in the future. The main reason is that the system's growth is still in its early stages. This section provides examples of how game theory, ontologies, artificial intelligence, and machine learning have been applied to security systems [13, 146].

11.9.1 ARTIFICIAL INTELLIGENCE

AI is being used in intrusion detection systems (IDS) more and more as the Internet of Things (IoT) increases security risk and job complexity. Due to the need for comprehensive plans and adaptable solutions to the quickly changing system, future ITS hacking will probably involve AI [146,147].

11.9.2 MACHINE LEARNING

The most often employed branch of artificial intelligence (AI) in cyber security systems is machine learning (ML). Its vulnerability during the training phase makes it weak. Hence the training dataset needs to be carefully chosen. The entire system may be jeopardized if noise is introduced (envison attacks, poisoning attacks). By proactive methods, a robust classifier must be built. Owing to this drawback, ML approaches are frequently utilized as a backup strategy [148]; reference [149] provides automated IP block listing using techniques from linear regression. Compared to human agents, the authors claim that it can minimize inaccurate block listing by about 90% and speed up removing problematic IPs.

11.9.3 ONTOLOGY

With unstructured data, ontology is a potential tool for addressing diverse problems. An emerging field is the use of ontology in the field of IoT security. Reference [150] describes an ontology for the Internet of Things data security. It is a common language for discussing the essential practical security aspects of data access and trade for producers, consumers, and intermediaries. Its objective is to provide relevant information on data gathering, handling, and use and on any laws that may pertain to it, certifications, and provenance.

11.9.4 GAME THEORY

Game theory is a powerful mathematical instrument successfully applied to privacy and cyber security [151]. Strategic decision making is studied in game theory, a field of mathematics. Game theory can be used in cyber security to evaluate

attacker and defender tactics and to model their behavior. There are some applications of game theory in defense [152]; in machine learning systems, the interactions between attackers and defenses can be modeled using adversarial machine learning. Cybersecurity Investment can be used to evaluate the investment strategies of organizations in cyber security by using robust machine learning models that can survive attacks created by defenders and then by understanding the tactics of the attackers. Game theory can assist businesses in deciding how much money to allocate to cyber security by simulating the behavior of attackers and defenses [153]. Intrusion detection can be used to model the behavior of attackers and defenders in intrusion detection systems. By understanding the strategies of attackers, defenders can design effective intrusion detection systems that can detect and respond to attacks. Cyber warfare can be used to model the behavior of nations in cyber warfare scenarios. By analyzing the strategies of different countries, game theory can help policymakers design effective cyber security policies and defense, and risk management can be used to analyze the risks associated with cyber security threats. By modeling the behavior of attackers and defenders, game theory can help organizations identify and mitigate risks associated with cyber security threats [154].

In reference [155], the suggested technique for identifying selfish nodes in MANETs combines reputation- and game-theory-based approaches. A clustered network comprises many phases played as games between nodes while delivering or forwarding data packets. Each player is allowed to choose whether to move the ball forward or not. The outcomes of the experiments have shown that the suggested method can successfully identify selfish and malicious nodes, decrease the data's end-to-end latency, and consume fewer node resources (energy, battery, memory, etc.). The proposed approach allows the self-centered and malicious nodes to cooperate and improve network performance [156].

11.10 CYBER RESILIENCE IN TRANSPORTATION: DESIGNING CYBER SECURITY FOR CONNECTED AND AUTONOMOUS MOBILITY

Connected and automated mobility covers the need to integrate cyber crime resilience into our future transportation systems and a concept of cyber security engineering [157]. To research the topic of cyber resilience, the Secure Cyber Systems Research Group (SCSRG) at WMG, located at the University of Warwick, was established in 1980 with an emphasis on manufacturing technology and industrial management (hence Warwick Manufacturing Group) [158]. Due to its size, WMG must occupy several buildings on the Warwick campus, which is located in central England, near the City of Coventry, the former epicenter of the UK's automobile manufacturing sector. WMG is a school that studies manufacturing and applied engineering, among other things (Jaguar Land Rover, Aston Martin, Dennis Eagle, etc.). WMG bridges the gap between academic and business research while developing the next crop of engineers, business managers, and technological leaders [159].

11.10.1 WHY CYBER SECURITY ENGINEERING IN CONNECTED AND AUTOMATED MOBILITY?

The implementation of automated mobility is underway, and connected and autonomous cars (CAVs) are already in use. Coventry City will soon have extremely light rail thanks to a partnership with the University of Warwick. In the area where the university is located, the firm Jaguar Land Rover makes a lot of electric vehicles. In addition, cars have a great deal of software-based capabilities and are networked. Cyber attacks, however, can target a software-controlled and networked equipment. How may cyber security risks be reduced in automobile engineering? That is the objective of the CAM cyber security engineering study [160].

11.10.2 TRANSPORTATION CYBER THREAT MOTIVATIONS

What propels the attacks on transportation infrastructure? The most typical one is monetary gain. The whole vehicle, its parts, and the commodities they transport are all stolen frequently because they are valuable. Vehicles will produce personalized datasets in the future, if not right now. Information is also valuable. Intellectual property (IP) has value, and a vehicle's engineering is attractive to thieves looking to steal IP [161]. Receiving free trips is an incentive for users of public transportation networks. Then there is the payment information for passengers, which is recorded in systems, and the card information needed to access transportation; both the personal and card information are essential. These are some illustrations of monetary hacking. Other hacking motives include vandalism and the desire to prove anything can be hacked. Through hacking, or hacktivism, militant activist organizations could attempt to make a point. Terrorists and nation-state actors both have the potential to attempt and spread mayhem by obstructing traffic, causing car accidents, and using moving targets as kinetic weapons. Listening to passengers' conversations while in a car has been done before. Attackers may want to take advantage of affluent and influential persons (VIPs) who ride in upscale vehicles [162]. A variety of threats can lead to attacks on transportation networks, which may be attacked for various causes, some of which are discussed next.

11.10.2.1 Financial Gain

Financial gain is one of the most common motivations behind cyber threats [163]. Cyber criminals can use various tactics to gain access to financial information or funds, including phishing scams, malware, and ransomware attack. Phishing scams involve sending phony emails that seem to be from a trustworthy source, like a bank or credit card business, to trick people into providing their financial information. Malware is a software class that harms or interferes with computer systems and can be used to steal login information or financial data. Malware, known as ransomware, encrypts a victim's computer or files and requires payment to unlock them [120]. Cyber criminals can also use tactics such as identity theft, credit card fraud, and bank fraud to gain access to financial information or funds. These tactics may involve stealing someone's personal information, using it to open fraudulent accounts or to make unauthorized purchases, or transferring funds from a victim's

statement to their own [164]. Overall, financial gain is a significant motivation for cyber threats, and individuals and organizations need to take steps to protect their financial information and assets from cyber attacks. This includes using strong passwords, regularly updating software and security systems, and being vigilant about suspicious emails or messages.

11.10.2.2 Vandalism

Vandalism as a cyber threat motivation is when an individual or group intentionally damages, defaces, or destroys digital assets or systems for malicious purposes [165]. Cyber vandalism is often motivated by a desire to cause disruption, gain attention, or express political or ideological views. Some examples of cyber vandalism include defacing websites with offensive content or political messages, deleting or altering files, spreading malware or viruses, and launching denial of service attacks to overwhelm and shut down websites or servers. Cyber vandalism can have severe repercussions, including monetary loss, reputational harm, and possible legal issues. People and groups must take precautions to safeguard their digital assets and systems, including using strong passwords, updating software, and installing security tools like firewalls and antivirus software. Law enforcement organizations and cyber security professionals also labor to locate and detain those responsible for cyber vandalism so that they can be held accountable for their deeds [166].

11.10.2.3 Hacktivism, Nation-State Actors, Terrorism

Hacktivism, nation-state actors, and terrorism are all potential motivations behind cyber threats:

- **Hacktivism:** Hacktivism refers to using hacking as a means to achieve political or social goals. Hacktivists often target government agencies, corporations, and other organizations that they believe are engaging in unethical or unjust practices. For example, the hacktivist group Anonymous has targeted organizations such as the Church of Scientology and the Ku Klux Klan [167].
- **Nation-State Actors:** Nation-state actors are government entities that engage in cyber attacks for political or economic gain. Nation-state actors can range from developed countries like the United States and China to smaller countries with advanced cyber capabilities. Nation-state actors often engage in espionage, stealing valuable intellectual property or state secrets, and in disruptive attacks on critical infrastructure.
- **Terrorism:** Terrorism is using violence or intimidation to achieve political or social goals. In recent years, terrorist groups have increasingly used the Internet to spread propaganda, recruit members, and plan attacks. Cyber attacks by terrorist groups may include hacking government websites, stealing sensitive information, and disrupting critical infrastructure [168].

All these motivations behind cyber threats pose a significant risk to individuals, organizations, and even entire nations. It is essential to be aware of these potential threats and take appropriate measures to protect against them.

11.10.2.4 Examples of Real-World Vehicle Cyber Issues

Vehicle hacks have happened in the past and are still happening today [169]. The relay attack is one of the more successful attacks on keyless car entry devices [170]. In this case, the car’s wireless key fob is stolen from the owner. The signal from a key fob inside a building will be received by an accomplice standing next to the vehicle using a communications system used by the thief. They can then get in the car, drive off, and depart. A distinct type of vehicle hacking is demonstrated by the Dieselgate emissions incident [171, 172].

11.10.3 HOW TO HACK TRANSPORTATION SYSTEMS

How might transportation systems be hacked? The techniques are akin to those used to compromise other systems, and they jeopardize the systems, software, and the confidentiality, integrity, and availability (CIA) of the data. Information system security may be breached by attacking the CIA triad [173]. We utilize fuzzing, penetration testing, vulnerability analysis, and conventional hacking approaches. Systems may have malware that is malicious programming. It is possible to spoof the signals and data the systems utilize (for example, for control). Attacks using denial of service are possible. Any form of computer-based system attacker is highly familiar with these techniques. Assault methods that can be used against vehicle systems are presented in Table 11.2 [174].

11.10.4 TRANSPORTATION ATTACK SURFACE AND ENGINEERING FALLIBILITY

Threat actors that might wish to target transportation systems have a broad attack surface in vehicles. There is an increase in the Internet- and cloud-based communications services integration into automobiles. These are utilized for services offered by vehicle manufacturers and are via cellular or Wi-Fi connections. Manufacturers are increasingly offering extra features like location-based services and remote diagnostics. Bluetooth is one of the local wireless vehicle communications interfaces. Systems for managing batteries and charging are included in electric and hybrid cars. Passengers that use transportation carry their gadgets and link them to moving cars. The automobile’s internal systems, in-vehicle control networks, control computers (ECUs), and all contemporary sensors are present.

TABLE 11.2
Assault Types That Can Be Employed Against Vehicle Systems

Traditional Hacking	Malicious Code	Malicious Code
Pen testing [175]	Malware	Replay
Vulnerability assessment [176]	(Phishing/virus/worm)	Falsification
Fuzzing [177]	Compromised/fake apps	Modification

Telematic systems are installed in vehicles to deliver services like fleet administration and insurance monitoring. With roadside infrastructure, vehicles are increasingly sharing warning information.

When developing and creating transportation products and services, it's important to take into account the various attack points that can be targeted. These attack points include everything from local car communications, charging and battery management systems, motors and actuators, and passenger/pedestrian devices like cellphones, tablets, and laptops connected to Internet, cloud, and data communications [162]. Particularly susceptible to assault are Wi-Fi hotspots and connections, as well as 3G/4G/5G cellular connections. The services manufacturers provide could also be a source of attack because they might not be adequately protected. Other possible targets for hackers include local vehicle communications like Bluetooth connections and vehicle to vehicle communication [178]. Charging and battery management systems, which are becoming increasingly important as more electric vehicles hit the market, can also be targeted. Hackers may try to manipulate the battery management system to cause a fire or explosion, for example. Motors and actuators control various vehicle functions and are potential attack points. Other potential targets are passenger and pedestrian devices, including smartphones, tablets, and laptops. Hackers may attempt to steal personal information or install malware through these devices. Aftermarket devices, such as GPS trackers and diagnostic tools, also represent potential vulnerabilities [179].

To attack the aforementioned, attackers search for engineering flaws. Consequently, it is essential to recognize human fallibility in engineering while creating systems. Engineering design complacency is what the attackers search for. In engineering, it is well-known that fallibility exists in various systems. One of the most common examples is the occurrence of bugs in software. Over several decades, engineers have faced multiple issues, such as backdoors, user errors, wrong configurations, vulnerabilities, and poor engineering practices. These issues can significantly damage the system, leading to downtime, financial loss, or even security breaches [180]. Backdoors are a type of vulnerability that allows unauthorized access to a system, compromising its integrity. User errors, on the other hand, can occur due to human mistakes, such as incorrectly entering data or making incorrect decisions. Wrong configurations can result in system failures, leading to significant downtime. Vulnerabilities are security flaws that hackers can exploit to gain unauthorized access to a system, causing substantial damage [181]. Poor engineering practices, such as failing to consider all potential use cases or not following proper design and testing procedures, can lead to system failures and other issues. It is essential to understand that these issues are not unique to any particular system or technology and can occur in any engineering project. As such, it is crucial to employ best practices and rigorous testing procedures to identify and mitigate potential issues early in development. How should we approach these problems in terms of transportation cyber security? Engineers working on transportation networks are retaliating. They employ cyber security experts, and automakers have set up bug bounty schemes. Penetration testing is performed on automobiles to identify any flaws that are subsequently rectified [182].

11.11 FUTURE OF CYBER SECURITY IN TRANSPORTATION SYSTEMS

11.11.1 EMERGING TECHNOLOGIES AND THEIR CYBER SECURITY IMPLICATIONS

Emerging technologies such as autonomous vehicles, drones, and smart transportation systems will present new cyber security challenges for transportation systems [183]. Organizations operating these systems must develop new strategies for securing these technologies against cyber threats [184].

11.11.2 REGULATORY AND POLICY CHANGES

Governments and regulatory bodies are likely to implement new policies and regulations to improve the cyber security of transportation systems. Organizations must stay informed about these changes and ensure compliance with new requirements [184].

11.11.3 INDUSTRY TRENDS

The transportation industry will likely see increased investment in cyber security measures in the coming years. This includes the development of new technologies and services aimed at improving the cyber security of transportation systems [184]. Overall, it is clear that cyber security attacks on transportation systems can have significant impacts on public safety, the economy, and organizational reputation. To prevent such attacks, organizations operating transportation systems should follow best practices for cyber security, develop a culture of cyber security awareness, implement risk management strategies, have an incident response plan, and collaborate with government, industry, and academia. Looking to the future, emerging technologies, policy changes, and industry trends are likely to shape the cyber security landscape of transportation systems in the years to come [185].

11.12 CONCLUSION

In conclusion, cyber attacks against ITS pose a significant threat to the safety and reliability of transportation networks. The increasing use of digital technologies in transportation systems has created new vulnerabilities that malicious actors can exploit to disrupt operations, steal data, or cause physical harm. Several types of cyber attacks, such as denial of service (DoS) attacks, ransomware attacks, and advanced persistent threats (APTs), can target ITS. These attacks can result in various consequences, from minor disruptions to catastrophic events that can cause significant economic and social damage. To prevent and mitigate cyber attacks against the ITS, it is essential to implement robust cyber security measures, including network segmentation, access control, encryption, and regular software updates. Additionally, stakeholders must adopt a risk-based approach to cyber security, identify potential threats and vulnerabilities, and implement appropriate countermeasures to reduce the risk of cyber attacks.

Given the critical role of ITS in modern transportation systems, it is vital to invest in cyber security research and development to improve the resilience of these systems. Collaboration among stakeholders, including government agencies, private companies, and academic institutions, can help address the complex and evolving nature of cyber threats to ITS.

REFERENCES

- [1] "Smart city challenge," no. U.S. Department of Transportation, 2017 [Online]. Available: <https://www.transportation.gov/smartycity>.
- [2] A. A. Ganin, A. C. Mersky, A. S. Jin, M. Kitsak, J. M. Keisler, and I. Linkov, "Resilience in intelligent transportation systems (ITS)," *Transp. Res. Part C Emerg. Technol.*, vol. 100, pp. 318–329, Mar. 2019, doi:10.1016/j.trc.2019.01.014.
- [3] V. Albino, U. Berardi, and R. M. Dangelico, "Smart cities: Definitions, dimensions, performance, and initiatives," *J. Urban Technol.*, vol. 22, no. 1, pp. 3–21, Jan. 2015, doi:10.1080/10630732.2014.942092.
- [4] J. C. Miles, "Intelligent transport systems: Overview and structure (History, Applications, and Architectures)," in *Encyclopedia of Automotive Engineering*, Chichester: John Wiley & Sons, Ltd, 2014, pp. 1–16. doi:10.1002/9781118354179.autol66.
- [5] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1624–1639, Dec. 2011, doi:10.1109/TITS.2011.2158001.
- [6] T. Mecheva and N. Kakanakov, "Cybersecurity in intelligent transportation systems," *Computers*, vol. 9, no. 4, p. 83, Oct. 2020, doi:10.3390/computers9040083.
- [7] L. Qi, "Research on intelligent transportation system technologies and applications," in *2008 Workshop on Power Electronics and Intelligent Transportation System*, 2008, IEEE, Guangzhou, China, pp. 529–531.
- [8] M. T. Riaz et al., "The intelligent transportation systems with advanced technology of sensor and network," in *2021 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube)*, 2021, pp. 1–6, doi:10.1109/ICECube53880.2021.9628331.
- [9] P. A. Mandhare, V. Kharat, and C. Y. Patil, "Intelligent road traffic control system for traffic congestion: A perspective," *Int. J. Comput. Sci. Eng.*, vol. 6, no. 7, p. 2018, 2018.
- [10] J. L. Adler and V. J. Blue, "Toward the design of intelligent traveler information systems," *Transp. Res. Part C Emerg. Technol.*, vol. 6, no. 3, pp. 157–172, Jun. 1998, doi:10.1016/S0968-090X(98)00012-6.
- [11] M. Han, S. Liu, S. Ma, and A. Wan, "Anonymous-authentication scheme based on fog computing for VANET," *PLoS ONE*, vol. 15, no. 2, p. e0228319, 2020.
- [12] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: A review of current applications and security solutions," *J. Cloud Comput.*, vol. 6, no. 1, pp. 1–22, 2017.
- [13] L. Cui, G. Xie, Y. Qu, L. Gao, and Y. Yang, "Security and privacy in smart cities: Challenges and opportunities," *IEEE Access*, vol. 6, pp. 46134–46145, 2018, doi:10.1109/ACCESS.2018.2853985.
- [14] Å. Holmner, K. L. Ebi, L. Lazuardi, and M. Nilsson, "Carbon footprint of telemedicine solutions-unexplored opportunity for reducing carbon emissions in the health sector," *PLoS ONE*, vol. 9, no. 9, p. e105040, 2014.
- [15] E. Akkartal and G. Y. Aras, "Sustainability in fleet management," *J. Adv. Res. Econ. Adm. Sci.*, vol. 2, no. 3, pp. 13–39, Sep. 2021, doi:10.47631/jareas.v2i3.288.

- [16] J. Guerrero-Ibáñez, S. Zeadally, and J. Contreras-Castillo, "Sensor technologies for intelligent transportation systems," *Sensors*, vol. 18, no. 4, p. 1212, Apr. 2018, doi:10.3390/s18041212.
- [17] T. Rawal and V. Devadas, "Intelligent transportation system in India—a review," *J. Manag. Dev.*, vol. 2, p. 299, 2015.
- [18] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017, doi:10.1016/j.vehcom.2017.01.002.
- [19] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for VANET," *Int. J. Netw. Secur. Its Appl.*, vol. 5, no. 5, p. 95, 2013.
- [20] T. Macaulay, *The 7 Deadly Threats to 4G*, 2013, McAfee, St. Clara, CA.
- [21] A. Mpitziopoulou, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Commun. Surv. Tutor.*, vol. 11, no. 4, pp. 42–56, 2009, doi:10.1109/SURV.2009.090404.
- [22] M. Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks," in *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2005, ACM, Alexandria, VA, USA, pp. 11–21.
- [23] V. H. La and A. R. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, 2014.
- [24] L. Song, Q. Han, and J. Liu, "Investigate key management and authentication models in VANETs," in *2011 International Conference on Electronics, Communications and Control (ICECC)*, Sep. 2011, pp. 1516–1519, doi:10.1109/ICECC.2011.6067807.
- [25] H. Sedjelmaci, M. Hadji, and N. Ansari, "Cyber security game for intelligent transportation systems," *IEEE Netw.*, vol. 33, no. 4, pp. 216–222, 2019.
- [26] D. A. S. Resul and M. Z. Gündüz, "Analysis of cyber-attacks in IoT-based critical infrastructures," *Int. J. Inf. Secur. Sci.*, vol. 8, no. 4, pp. 122–133, 2020.
- [27] J. Harding et al., "Vehicle-to-vehicle communications: Readiness of V2V technology for application," United States, National Highway Traffic Safety Administration, 2014. <https://rosap.ntl.bts.gov/view/dot/27999>
- [28] M. El Zorkany, A. Yasser, and A. I. Galal, "Vehicle to vehicle 'V2V' communication: Scope, importance, challenges, research directions and future," *Open Transp. J.*, vol. 14, no. 1, 2020.
- [29] A. Faisal, M. Kamruzzaman, T. Yigitcanlar, and G. Currie, "Understanding autonomous vehicles," *J. Transp. Land Use*, vol. 12, no. 1, pp. 45–72, 2019.
- [30] E. Yurtsever, J. Lambert, A. Carballo, and K. Takeda, "A survey of autonomous driving: Common practices and emerging technologies," *IEEE Access*, vol. 8, pp. 58443–58469, 2020.
- [31] X. Sun, F. R. Yu, and P. Zhang, "A survey on cyber-security of connected and autonomous vehicles (CAVs)," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6240–6259, 2021.
- [32] Y. Wang, L. Kung, and T. A. Byrd, "Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations," *Technol. Forecast. Soc. Change*, vol. 126, pp. 3–13, 2018.
- [33] M. A. Memon, S. Soomro, A. K. Jumani, and M. A. Kartio, "Big data analytics and its applications," *arXiv Prepr. arXiv1710.04135*, 2017.
- [34] L. Figueiredo, I. Jesus, J. A. T. Machado, J. R. Ferreira, and J. L. M. De Carvalho, "Towards the development of intelligent transportation systems," in *ITSC 2001. 2001 IEEE Intelligent Transportation Systems. Proceedings (Cat. No. O1TH8585)*, 2001, IEEE, Oakland, CA, USA, pp. 1206–1211.
- [35] M. Antonakakis et al., "Understanding the mirai botnet," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, Usenix Association, Vancouver, BC, Canada, pp. 1093–1110.

- [36] H. Hasbullah and I. A. Soomro, "Denial of service (DOS) attack and its possible solutions in VANET," *Int. J. Electron. Commun. Eng.*, vol. 4, no. 5, pp. 813–817, 2010.
- [37] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure internet of things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019.
- [38] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, 2011, ACM, Chicago, Illinois, USA, pp. 75–86.
- [39] L. Li, P. L. Correia, and A. Hadid, "Face recognition under spoofing attacks: Countermeasures and research directions," *IET Biometrics*, vol. 7, no. 1, pp. 3–14, 2018.
- [40] B. Bhushan, G. Sahoo, and A. K. Rai, "Man-in-the-middle attack in wireless and computer networking—A review," in *2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall)*, 2017, IEEE, Dehradun, India, pp. 1–6.
- [41] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of prevention schemes for man-in-the-middle (MITM) attack in vehicular ad hoc networks," *Int. J. Eng. Manag. Res.*, vol. 10, 2020.
- [42] A. Becher, Z. Benenson, and M. Dornseif, "Tampering with notes: Real-world physical attacks on wireless sensor networks," in *Security in Pervasive Computing: Third International Conference, SPC 2006, York, UK, April 18–21, 2006. Proceedings 3*, 2006, Springer, Berlin, Heidelberg, pp. 104–118.
- [43] S. Paley, T. Hoque, and S. Bhunia, "Active protection against PCB physical tampering," in *2016 17th International Symposium on Quality Electronic Design (ISQED)*, 2016, IEEE, Santa Clara, California, USA, pp. 356–361.
- [44] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, 2019.
- [45] F. J. Martinez, C.-K. Toh, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Emergency services in future intelligent transportation systems based on vehicular communication networks," *IEEE Intell. Transp. Syst. Mag.*, vol. 2, no. 2, pp. 6–20, 2010.
- [46] D. I. Robertson and R. D. Bretherton, "Optimizing networks of traffic signals in real time—the SCOOT method," *IEEE Trans. Veh. Technol.*, vol. 40, no. 1, pp. 11–15, 1991.
- [47] A. Ziebinski, R. Cupek, D. Grzechca, and L. Chruszczyk, "Review of advanced driver assistance systems (ADAS)," in *AIP Conference Proceedings*, 2017, AIP Publishing, vol. 1906, no. 1, p. 120002, Bydgoszcz, Poland.
- [48] K. C. Dey, A. Rayamajhi, M. Chowdhury, P. Bhavsar, and J. Martin, "Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network—Performance evaluation," *Transp. Res. Part C Emerg. Technol.*, vol. 68, pp. 168–184, 2016.
- [49] D. Levinson and E. Chang, "A model for optimizing electronic toll collection systems," *Transp. Res. Part A Policy Pract.*, vol. 37, no. 4, pp. 293–314, 2003.
- [50] F. I. Shaikh, P. N. Jadhav, S. P. Bandarkar, O. P. Kulkarni, and N. B. Shardoor, "Smart parking system based on embedded system and sensor network," *Int. J. Comput. Appl.*, vol. 140, no. 12, 2016.
- [51] S. Kwatiray, J. Almhana, and Z. Liu, "Adaptive traffic light control using VANET: A case study," in *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, Jul. 2013, pp. 752–757, doi:10.1109/IWCMC.2013.6583651.
- [52] A. Raza et al., "Evaluation of a sustainable urban transportation system in terms of traffic congestion—A case study in Taxila, Pakistan," *Sustainability*, vol. 14, no. 19, p. 12325, Sep. 2022, doi:10.3390/su141912325.
- [53] Y. Wang, X. Yang, H. Liang, and Y. Liu, "A review of the self-adaptive traffic signal control system based on future traffic environment," *J. Adv. Transp.*, vol. 2018, 2018.

- [54] J. Li, Y. Zhang, and Y. Chen, "A self-adaptive traffic light control system based on speed of vehicles," in *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 2016, IEEE, Vienna, Austria, pp. 382–388.
- [55] D. Tian, G. Wu, K. Boriboonsomsin, and M. J. Barth, "Performance measurement evaluation framework and co-benefit/tradeoff analysis for connected and automated vehicles (CAV) applications: A survey," *IEEE Intell. Transp. Syst. Mag.*, vol. 10, no. 3, pp. 110–122, 2018.
- [56] J. C. Muñoz, J. Soza-Parra, and S. Raveau, "A comprehensive perspective of unreliable public transport services' costs," *Transp. A Transp. Sci.*, vol. 16, no. 3, pp. 734–748, 2020.
- [57] D. Vakula and B. Raviteja, "Smart public transport for smart cities," in *2017 International Conference on Intelligent Sustainable Systems (ICISS)*, 2017, IEEE, Palladam, India, pp. 805–810.
- [58] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, 2016, IEEE, Rio de Janeiro, Brazil, pp. 2663–2668.
- [59] J. Miller, "Vehicle-to-vehicle-to-infrastructure (V2V2I) intelligent transportation system architecture," in *2008 IEEE Intelligent Vehicles Symposium*, 2008, IEEE, Eindhoven, The Netherlands, pp. 715–720.
- [60] G. S. Tewolde, "Sensor and network technology for intelligent transportation systems," in *2012 IEEE International Conference on Electro/Information Technology*, 2012, IEEE, Indianapolis, Indiana, USA, pp. 1–7.
- [61] Y. Demchenko, C. De Laat, and P. Membrey, "Defining architecture components of the Big Data Ecosystem," in *2014 International Conference on Collaboration Technologies and Systems (CTS)*, 2014, IEEE, Minneapolis, Minnesota, USA, pp. 104–112.
- [62] A. Fehske, G. Fettweis, J. Malmodin, and G. Biczok, "The global footprint of mobile communications: The ecological and economic perspective," *IEEE Commun. Mag.*, vol. 49, no. 8, pp. 55–62, 2011.
- [63] M. Zaminkar, F. Sarkohaki, and R. Fotohi, "A method based on encryption and node rating for securing the RPL protocol communications in the IoT ecosystem," *Int. J. Commun. Syst.*, vol. 34, no. 3, p. e4693, 2021.
- [64] P. Manikonda, A. K. Yerrapragada, and S. S. Annasamudram, "Intelligent traffic management system," in *2011 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (STUDENT)*, 2011, IEEE, Semenyih, Selangor, Malaysia, pp. 119–122.
- [65] K. Sjoberg, P. Andres, T. Buburuzan, and A. Brakemeier, "Cooperative intelligent transport systems in Europe: Current deployment status and outlook," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 89–97, 2017.
- [66] A. Demba and D. P. F. Möller, "Vehicle-to-vehicle communication technology," in *2018 IEEE International Conference on Electro/Information Technology (EIT)*, 2018, pp. 459–464.
- [67] C. Bergenheim, E. Hedin, and D. Skarin, "Vehicle-to-vehicle communication for a platooning system," *Procedia Soc. Behav. Sci.*, vol. 48, pp. 1222–1233, 2012.
- [68] A. Ibraeva and J. F. de Sousa, "Marketing of public transport and public transport information provision," *Procedia Soc. Behav. Sci.*, vol. 162, pp. 121–128, Dec. 2014, doi:10.1016/j.sbspro.2014.12.192.
- [69] C. A. Klöckner and A. Blöbaum, "A comprehensive action determination model: Toward a broader understanding of ecological behaviour using the example of travel mode choice," *J. Environ. Psychol.*, vol. 30, no. 4, pp. 574–586, 2010.
- [70] F. Jaehn, "Sustainable operations," *Eur. J. Oper. Res.*, vol. 253, no. 2, pp. 243–264, 2016.

- [71] K. N. Qureshi and A. H. Abdullah, "A survey on intelligent transportation systems," *Middle-East J. Sci. Res.*, vol. 15, no. 5, pp. 629–642, 2013.
- [72] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing sensor to cloud ecosystem using internet of things (IoT) security framework," in *Proceedings of the International Conference on Internet of things and Cloud Computing*, 2016, ACM, Cambridge, United Kingdom, pp. 1–5.
- [73] J. L. Hernández-Ramos, A. J. Jara, L. Marin, and A. F. Skarmeta, "Distributed capability-based access control for the internet of things," *J. Internet Serv. Inf. Secur.*, vol. 3, no. 3/4, pp. 1–16, 2013.
- [74] I. Lungu and A. Tăbușcă, "Optimizing anti-phishing solutions based on user awareness, education and the use of the latest web security solutions," *Inform. Econ.*, vol. 14, no. 2, 2010.
- [75] M. Spradling and J. Straub, "Evaluation of elements of a prospective system to alert users to intentionally deceptive content," in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2020, pp. 224–229, doi:10.1109/CSCI51800.2020.00045.
- [76] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, 2019, doi:10.1109/TITS.2018.2815678.
- [77] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, p. e0155781, 2016.
- [78] L. Chen et al., "BDS-3 integrity risk modeling and probability evaluation," *Remote Sens.*, vol. 14, no. 4, p. 944, Feb. 2022, doi:10.3390/rs14040944.
- [79] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, and P. Burnap, "A supervised intrusion detection system for smart home IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9042–9053, Oct. 2019, doi:10.1109/JIOT.2019.2926365.
- [80] I. Aguirre and S. Alonso, "Improving the automation of security information management: A collaborative approach," *IEEE Secur. Priv.*, vol. 10, no. 1, pp. 55–59, 2011.
- [81] H. Kılıç, N. S. Katal, and A. A. Selçuk, "Evasion techniques efficiency over the IPS/IDS technology," in *2019 4th International Conference on Computer Science and Engineering (UBMK)*, 2019, IEEE, Samsun, Turkey, pp. 542–547.
- [82] Y. M. Tashtoush et al., "Agile approaches for cybersecurity systems, IoT and intelligent transportation," *IEEE Access*, vol. 10, pp. 1360–1375, 2021.
- [83] D. Schmitt, V. Gollnick, D. Schmitt, and V. Gollnick, *The Air Transport System*, Vienna: Springer, 2016.
- [84] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *J. Organ. Comput. Electron. Commer.*, vol. 28, no. 3, pp. 269–282, Jul. 2018, doi:10.1080/10919392.2018.1484598.
- [85] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustain. Cities Soc.*, vol. 50, p. 101660, Oct. 2019, doi:10.1016/j.scs.2019.101660.
- [86] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 998–1010, 2012.
- [87] C. W. Probst, J. Huncker, M. Bishop, and D. Gollmann, *Insider Threats in Cyber Security*, vol. 49, New York, NY: Springer, 2010.
- [88] G. E. I. Selim, E. Z. Z. E.-D. Hemdan, A. M. Shehata, and N. A. El-Fishawy, "Anomaly events classification and detection system in critical industrial internet of things infrastructure using machine learning algorithms," *Multimed. Tools Appl.*, vol. 80, pp. 12619–12640, 2021.

- [89] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications [Topics in Automotive Networking]," *IEEE Commun. Mag.*, vol. 48, no. 5, pp. 156–162, May 2010, doi:10.1109/MCOM.2010.5458377.
- [90] C. Maple, "Security and privacy in the internet of things," *J. Cyber Policy*, vol. 2, no. 2, pp. 155–184, May 2017, doi:10.1080/23738871.2017.1366536.
- [91] A. Gelman, A. Jarrot, A. He, J. Kherroubi, and R. Laronga, "Borehole image correspondence and automated alignment," in *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2017, pp. 1807–1811, doi:10.1109/ICASSP.2017.7952468.
- [92] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer (Long. Beach. Calif.)*, vol. 35, no. 10, pp. 54–62, 2002.
- [93] J. P. Tailor and A. D. Patel, "A comprehensive survey: Ransomware attacks prevention, monitoring and damage control," *Int. J. Res. Sci. Innov.*, vol. 4, no. 15, pp. 116–121, 2017.
- [94] A. Mačiulis, A. V. Vasiliauskas, and G. Jakubauskas, "The impact of transport on the competitiveness of national economy," *Transport*, vol. 24, no. 2, pp. 93–99, 2009.
- [95] L.-G. Mattsson and E. Jenelius, "Vulnerability and resilience of transport systems—A discussion of recent research," *Transp. Res. Part A Policy Pract.*, vol. 81, pp. 16–34, Nov. 2015, doi:10.1016/j.tra.2015.06.002.
- [96] C. G. L. Krishna, and R. R. Murphy, "A review on cybersecurity vulnerabilities for unmanned aerial vehicles," in *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*, 2017, IEEE, Shanghai, China, pp. 194–199.
- [97] M. D. Cavelti, "Critical information infrastructure: Vulnerabilities, threats and responses," *Disarm. Forum*, vol. 3, pp. 15–22, 2007.
- [98] A. R. Hale, J. Stoop, and J. Hommels, "Human error models as predictors of accident scenarios for designers in road transport systems," *Ergonomics*, vol. 33, no. 10–11, pp. 1377–1387, 1990.
- [99] S. Keay and S. Kirby, "Defining vulnerability: From the conceptual to the operational," *Polic. J. Policy Pract.*, vol. 12, no. 4, pp. 428–438, 2018.
- [100] F. Ullah, M. Edwards, R. Ramdhany, R. Chitchyan, M. A. Babar, and A. Rashid, "Data exfiltration: A review of external attack vectors and countermeasures," *J. Netw. Comput. Appl.*, vol. 101, pp. 18–54, 2018.
- [101] D. Gillman, Y. Lin, B. Maggs, and R. K. Sitaraman, "Protecting websites from attack with secure delivery networks," *Computer (Long. Beach. Calif.)*, vol. 48, no. 4, pp. 26–34, 2015.
- [102] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity," in *2015 International Conference on Cyberspace (CYBER-Abuja)*, 2015, IEEE, Abuja, Nigeria, pp. 91–100.
- [103] M. Badra, S. El-Sawda, and I. Hajjeh, "Phishing attacks and solutions," in *Proceedings of 3rd International ICST Conference on Mobile Multimedia Communications*, 2010, European Union Digital Library, Oulu, Finland.
- [104] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: State of the art and future challenges," *Neural Comput. Appl.*, vol. 28, pp. 3629–3654, 2017.
- [105] A. Zimba, Z. Wang, and H. Chen, "Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems," *ICT Express*, vol. 4, no. 1, pp. 14–18, Mar. 2018, doi:10.1016/j.ict.2017.12.007.
- [106] A. Haydari and Y. Yilmaz, "Real-time detection and mitigation of DDoS attacks in intelligent transportation systems," in *2018 21st International Conference on*

- Intelligent Transportation Systems (ITSC)*, Nov. 2018, IEEE, pp. 157–163, doi:10.1109/ITSC.2018.8569698.
- [107] H. Aldawood and G. Skinner, “An advanced taxonomy for social engineering attacks,” *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 1–11, 2020.
- [108] L. E. Funderburg, H. Ren, and I.-Y. Lee, “Pairing-free signatures with insider-attack resistance for Vehicular Ad-Hoc Networks (VANETs),” *IEEE Access*, vol. 9, pp. 159587–159597, 2021, doi:10.1109/ACCESS.2021.3131189.
- [109] H. F. Atlam and G. B. Wills, “IoT security, privacy, safety and ethics,” in *Digital Twin Technologies and Smart Cities*, pp. 123–149, 2020, doi:10.1007/978-3-030-18732-3_8.
- [110] I. Ashraf et al., “A survey on cyber security threats in IoT-enabled maritime industry,” *IEEE Trans. Intell. Transp. Syst.*, pp. 1–14, 2022, doi:10.1109/TITS.2022.3164678.
- [111] R. Brewer, “Ransomware attacks: Detection, prevention and cure,” *Netw. Secur.*, vol. 2016, no. 9, pp. 5–9, 2016.
- [112] B. Ranabhat, J. Clements, J. Gatlin, K.-T. Hsiao, and M. Yampolskiy, “Optimal sabotage attack on composite material parts,” *Int. J. Crit. Infrastruct. Prot.*, vol. 26, p. 100301, 2019.
- [113] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel, “The economic impact of cyber-attacks,” *Congr. Res. Serv. Doc. CRS RL32331 (Washingt, DC)*, vol. 2, 2004.
- [114] S. Parkinson, P. Ward, K. Wilson, and J. Miller, “Cyber threats facing autonomous and connected vehicles: Future challenges,” *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, 2017.
- [115] L. R. Shapiro, M.-H. Maras, L. Velotti, S. Pickman, H.-L. Wei, and R. Till, “Trojan horse risks in the maritime transportation systems sector,” *J. Transp. Secur.*, vol. 11, pp. 65–83, 2018.
- [116] Q. He, X. Meng, and R. Qu, “Towards a severity assessment method for potential cyber attacks to connected and autonomous vehicles,” *J. Adv. Transp.*, vol. 2020, pp. 1–15, 2020.
- [117] K. Beaver, *Hacking for Dummies*, Indiana: John Wiley & Sons, 2007.
- [118] S. Traer and P. Bednar, “Motives behind DDOS attacks,” in *Digital Transformation and Human Behavior: Innovation for People and Organisations*, 2021, Springer International Publishing, pp. 135–147.
- [119] C. A. Meyers, S. S. Powers, and D. M. Faissol, “Taxonomies of cyber adversaries and attacks: A survey of incidents and approaches,” in *Lawrence Livermore National Lab (LLNL)*, Livermore, CA, 2009.
- [120] P. Warren, K. Kaivanto, and D. Prince, “Could a cyber attack cause a systemic impact in the financial sector?,” *Bank Engl. Q. Bull.*, vol. 58, no. 4, pp. 21–30, 2019.
- [121] E. Iasiello, “Cyber attack: A dull tool to shape foreign policy,” in *2013 5th International Conference on Cyber Conflict (CYCON 2013)*, 2013, IEEE, Tallinn, Estonia, pp. 1–18.
- [122] M. Ulsch, *Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks*, Indiana: Wiley Online Library, 2014.
- [123] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. G. Gourisetti, “Cyber threat dictionary using mitre attack matrix and NIST cybersecurity framework mapping,” in *2020 Resilience Week (RWS)*, 2020, IEEE, Salt Lake City, Utah, USA, pp. 106–112.
- [124] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” *Comput. Secur.*, vol. 30, no. 8, pp. 719–731, Nov. 2011, doi:10.1016/j.cose.2011.08.004.
- [125] M. Kenney, “Cyber-terrorism in a post-stuxnet world,” *Orbis*, vol. 59, no. 1, pp. 111–128, 2015.
- [126] F. Palmieri, S. Ricciardi, U. Fiore, M. Ficco, and A. Castiglione, “Energy-oriented denial of service attacks: An emerging menace for large cloud infrastructures,” *J. Supercomput.*, vol. 71, pp. 1620–1641, 2015.

- [127] M. Westerlund, "The emergence of deepfake technology: A review," *Technol. Innov. Manag. Rev.*, vol. 9, no. 11, 2019.
- [128] J. Valente, *Dracula's Crypt: Bram Stoker, Irishness, and the Question of Blood*, USA: University of Illinois Press, Urbana, USA, 2002.
- [129] E. Ben Hamida, H. Noura, and W. Znaidi, "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures," *Electronics*, vol. 4, no. 3, pp. 380–423, 2015.
- [130] M. S. Uddin, M. M. Ahmed, J. B. Alam, and M. Islam, "Smart anti-theft vehicle tracking system for Bangladesh based on internet of things," in *2017 4th International Conference on Advances in Electrical Engineering (ICAEE)*, 2017, IEEE, Dhaka, Bangladesh, pp. 624–628.
- [131] V. K. Sadagopan, U. Rajendran, and A. J. Francis, "Anti theft control system design using embedded system," in *Proceedings of 2011 IEEE International Conference on Vehicular Electronics and Safety*, 2011, IEEE, Beijing, China, pp. 1–5.
- [132] P. Singh, T. Sethi, B. B. Biswal, and S. K. Pattanayak, "A smart anti-theft system for vehicle security," *Int. J. Mater. Mech. Manuf.*, vol. 3, no. 4, pp. 249–254, 2015.
- [133] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, "Hacker types, motivations and strategies: A comprehensive framework," *Comput. Hum. Behav. Rep.*, vol. 5, p. 100167, Mar. 2022, doi:10.1016/j.chbr.2022.100167.
- [134] D. E. Denning, "The ethics of cyber conflict," *Handb. Inf. Comput. Ethics*, pp. 407–428, 2008.
- [135] G. M. Makrakis, C. Koliass, G. Kambourakis, C. Rieger, and J. Benjamin, "Industrial and critical infrastructure security: Technical analysis of real-life security incidents," *IEEE Access*, vol. 9, pp. 165295–165325, 2021.
- [136] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electr. Inf. Shar. Anal. Cent.*, vol. 388, pp. 1–29, 2016.
- [137] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A master attack methodology for an AI-based automated attack planner for smart cities," *IEEE Access*, vol. 6, pp. 48360–48373, 2018.
- [138] K. Kraszewski, "SamSam and the silent battle of Atlanta," in *2019 11th International Conference on Cyber Conflict (CyCon)*, 2019, IEEE, Tallinn, Estonia, vol. 900, pp. 1–16.
- [139] S. Mansfield-Devine, "Ransomware: The most popular form of attack," *Comput. Fraud Secur.*, vol. 2017, no. 10, pp. 15–20, Oct. 2017, doi:10.1016/S1361-3723(17)30092-1.
- [140] M. Taddeo, "Three ethical challenges of applications of artificial intelligence in cybersecurity," *Minds Mach.*, vol. 29, no. 2, pp. 187–191, 2019, doi:10.1007/s11023-019-09504-8.
- [141] S. Ghafur, E. Grass, N. R. Jennings, and A. Darzi, "The challenges of cybersecurity in health care: The UK National Health Service as a case study," *Lancet Digit. Heal.*, vol. 1, no. 1, pp. e10–e12, 2019.
- [142] A. Ioanid, C. Scarlat, and G. Militaru, "The effect of cybercrime on Romanian SMEs in the context of WannaCry ransomware attacks," in *European Conference on Innovation and Entrepreneurship*, 2017, Academic Conferences International Limited, Paris, France, pp. 307–313.
- [143] P. K. Kerr, J. Rollins, and C. A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Washington, DC: Congressional Research Service, 2010.
- [144] Y. Katz and W. Jpost, "Stuxnet virus set back Iran's nuclear program by 2 years," *Jerusalem Post*, vol. 15, 2010.
- [145] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010," *Strategy Insights*, Spring 2011.
- [146] S. Aldhaheri, D. Alghazzawi, L. Cheng, B. Alzahrani, and A. Al-Barakati, "DeepDCA: Novel network-based detection of IoT attacks using artificial immune system," *Appl. Sci.*, vol. 10, no. 6, p. 1909, Mar. 2020, doi:10.3390/app10061909.

- [147] T. de J. Mateo Sanguino, J. M. Lozano Domínguez, and P. de Carvalho Baptista, “Cybersecurity certification and auditing of automotive industry,” pp. 95–124, 2020. doi:10.1016/bs.atpp.2020.01.002.
- [148] N. Rahimi, J. Maynor, and B. Gupta, “Adversarial machine learning: Difficulties in applying machine learning to existing cybersecurity systems,” in *Proceedings of 35th International Conference on Computers and their Applications*, EPIc Series in Computing, vol. 69, pp. 40–47 EasyChair Proceedings in Computing (EPIc), San Francisco, CA, USA, 2020.
- [149] D. Jeon and B. Tak, “BlackEye: Automatic IP blacklisting using machine learning from security logs,” *Wirel. Netw.*, vol. 28, no. 2, pp. 937–948, 2022, doi:10.1007/s11276-019-02201-5.
- [150] P. Gonzalez-Gil, J. A. Martinez, and A. F. Skarmeta, “Lightweight data-security ontology for IoT,” *Sensors*, vol. 20, no. 3, p. 801, Feb. 2020, doi:10.3390/s20030801.
- [151] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, “A survey of game theoretic methods for cyber security,” in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*, Jun. 2016, pp. 631–636, doi:10.1109/DSC.2016.90.
- [152] S. Lipovetsky and M. Conklin, “Analysis of regression in game theory approach,” *Appl. Stoch. Model. Bus. Ind.*, vol. 17, no. 4, pp. 319–330, 2001.
- [153] S. Musman and A. Turner, “A game theoretic approach to cyber security risk management,” *J. Def. Model. Simul.*, vol. 15, no. 2, pp. 127–146, 2018.
- [154] X. Liang and Y. Xiao, “Game theory for network security,” *IEEE Commun. Surv. Tutor.*, vol. 15, no. 1, pp. 472–486, 2012.
- [155] S. Nobahary, H. G. Garakani, A. Khademzadeh, and A. M. Rahmani, “Selfish node detection based on hierarchical game theory in IoT,” *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–19, 2019.
- [156] C. T. Do et al., “Game theory for cyber security and privacy,” *ACM Comput. Surv.*, vol. 50, no. 2, pp. 1–37, 2017.
- [157] Ó. Castillo Campo, V. Gayoso Martínez, L. Hernández Encinas, A. Martín Muñoz, and R. Álvarez Fernández, “State of the art of cybersecurity in cooperative, connected and automated mobility,” pp. 104–113, 2023, doi:10.1007/978-3-031-18409-3_11.
- [158] K. Neupane, R. Haddad, and L. Chen, “Next Generation Firewall for Network Security: A Survey,” in *SoutheastCon 2018*, 2018, St. Petersburg, FL, USA, pp. 1–6, 2018.
- [159] D. S. Ray, “Cyber-resilient connected autonomous vehicles,” University of Florida Transportation Institute, May 2021 [Online]. Available: <https://www.transportation.institute.ufl.edu/2021/05/cyber-resilient-connected-autonomous-vehicles/>.
- [160] “Capri Consortium. Connected and automated vehicles,” 2020 [Online]. Available: <https://caprimobility.exhibition.app/>.
- [161] R. Taplin, *Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA*, USA: Routledge, New York, USA, 2020.
- [162] D. S. Fowler, “Cybersecurity engineering in connected and automated mobility: Cyber resilience in transportation,” in *Cyber Security Summit Brazil 2021–28th and 29th September 2021*, <https://www.cybersecuritysummit.com.br/>.
- [163] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, “How blockchain can impact financial services—The overview, challenges and recommendations from expert interviewees,” *Technol. Forecast. Soc. Change*, vol. 158, p. 120166, Sep. 2020, doi:10.1016/j.techfore.2020.120166.
- [164] A. F. Altwairqi, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri, “Four most famous cyber attacks for financial gains,” *Int. J. Eng. Adv. Technol.*, vol. 9, pp. 2131–2139, 2019.
- [165] G. Kaur, Z. Habibi Lashkari, A. Habibi Lashkari, G. Kaur, Z. Habibi Lashkari, and A. Habibi Lashkari, “Cybersecurity threats in FinTech,” *Underst. Cybersec. Manag. FinTech Challenges, Strateg. Trends*, pp. 65–87, 2021.

- [166] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*, 2015, IEEE, Fort Lauderdale, Florida, USA, pp. 1–6.
- [167] J. L. Beyer, "Trolls and Hacktivists," *Oxford Handb. Digit. Media Sociol.*, p. 417, 2022.
- [168] M. R. Shad, "Cyber threat landscape and readiness challenge of Pakistan," *Strateg. Stud.*, vol. 39, no. 1, pp. 1–19, 2019.
- [169] D. S. Fowler, *Automotive Cyber Security Timeline*, Tek Eye, 2020, <https://tekeye.uk/automotive/cyber-security/timeline>, 2021.
- [170] A. Francillon, B. Danev, and S. Capkun, "Relay attacks on passive keyless entry and start systems in modern cars," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2011, Eidgenössische Technische Hochschule Zürich, Department of Computer Science.
- [171] M. Contag et al., "How they did it: An analysis of emission defeat devices in modern automobiles," in *2017 IEEE Symposium on Security and Privacy (SP)*, May 2017, pp. 231–250, doi:10.1109/SP.2017.66.
- [172] "Wikimedia commons," VW Golf TDI Clean Diesel, 2010 [Online]. Available: https://commons.wikimedia.org/wiki/File:VW_Golf_TDI_Clean_Diesel_WAS_2010_8982.JPG.
- [173] K. B. Kelarestaghi, K. Heaslip, M. Khalilikhah, A. Fuentes, and V. Fessmann, "Intelligent transportation system security: Hacked message signs," *SAE Int. J. Transp. Cybersecur. Priv.*, vol. 1, no. 11-01-02-0004, pp. 75–90, 2018.
- [174] The MIT Gallery of Hacks, "This sign has been hacked," 2007 [Online]. Available: http://hacks.mit.edu/Hacks/by_year/2007/sign_hacked/.
- [175] P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, Netherlands: Elsevier, 2013.
- [176] S. Shah and B. M. Mehtre, "An overview of vulnerability assessment and penetration testing techniques," *J. Comput. Virol. Hacking Tech.*, vol. 11, pp. 27–49, 2015.
- [177] P. Godefroid, "Fuzzing: Hack, art, and science," *Commun. ACM*, vol. 63, no. 2, pp. 70–76, 2020.
- [178] S. Wheatley, T. Maillart, and D. Sornette, "The extreme risk of personal data breaches and the erosion of privacy," *Eur. Phys. J. B*, vol. 89, pp. 1–12, 2016.
- [179] R. Horak, *Telecommunications and Data Communications Handbook*, Indiana: John Wiley & Sons, 2007.
- [180] N. C. Rowe and E. J. Custy, "Deception in cyber attacks," in *Cyber Warfare and Cyber Terrorism*, pp. 91–96, IGI Global, Hershey, Pennsylvania, USA, 2007.
- [181] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, IEEE, Gaithersburg, MD, US, pp. 244–249.
- [182] "Tencent keen security lab. Experimental security assessment of BMW cars: A summary report," 2018 [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf.
- [183] J. Guerrero-Ibañez, J. Contreras-Castillo, and S. Zeadally, "Deep learning support for intelligent transportation systems," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 3, p. e4169, 2021.
- [184] H. P. Dai Nguyen and R. Zoltán, "The current security challenges of vehicle communication in the future transportation system," in *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*, 2018, IEEE, Subotica, Serbia, pp. 161–166.
- [185] M. Benyahya, A. Collen, S. Kechagia, and N. A. Nijdam, "Automated city shuttles: Mapping the key challenges in cybersecurity, privacy and standards to future developments," *Comput. Secur.*, vol. 122, p. 102904, 2022.

12 Intelligent Transportation Systems for IoT-Based UAV Networks

Mamoona Jamil, Usman Haider, Inam Ullah Khan, and Tarandeep Kaur Bhatia

12.1 INTRODUCTION

In this era, systems have changed in trendy ways. The study field of intelligent transportation systems (ITS) has flourished not only in the industrial sector but also in the military sector. Its autonomous features have advantages throughout the mobile generations. Intelligent transportation system (ITS) is a well-known system in transportation control. This system manages work logically. In the literature, this well-known smart technology detects all problems and solves them wisely [1]. Additionally, with the easy deployment of unmanned aerial vehicle (UAV) traffic, all networks can be covered by ubiquitous connectivity in space, air, and land, as well as underwater [2]. Another promising field in which researchers are more interested is artificial intelligence (AI). Thanks to this fruitful collection of studies, many dynamic problems are being solved by this area of study [3]. Like a smart IoT grid, the hands-on, self-aware prediction of a statistical neural network, self-managing and hands-on knowledge-based decisions of a compound nature are made [4]. Additionally, AI can perform efficiently compared to prediction algorithm methods [5].

UAV networks highlight the key features in high-mobility communication areas—in telecommunications, data processing, navigation systems—and serve many emerging applications, where a large amount of data is being processed [6]. Incorporation of machine-to-machine, machine-to-backbone infrastructure, and blockchain peer-to-peer augmentation in the field of UAV networks, enables such networks to work efficiently in applications like search and rescue operations in the case of disaster scenarios like earthquakes or jungle fire or patrolling for weather monitoring with respect to climate change and farming [7, 8]. Rescue can take the form of drone networks and autopilot flying ad hoc networks. Moreover, the characteristics of a small Compaq drone enable it to fly easily in spaces without incurring much cost and using much infrastructure using a cellular vehicle to the IoT [2].

Ad hoc drone networks in IoT worked better with limited resources with AI and quality of services (QoS), contained low latency rate, minimized energy consumption, and easily communicated with other smart environmental devices in an unfriendly environment [9]. A small paradigm of the IoT feature objective is

sufficient to improve the quality of citizens' lives; it has made the services of drones fast and easily applicable in indoor and outdoor environments. However, security and privacy in the systems have significant challenges [10]. There is a plethora of research work in the industrial domain as well as in academia, but some problems still need to be discussed in the contributions of the earliest research work.

The main subject facing technology is to attain compatibility with the sixth generation; computer applications need to deal with the diversity of constraints with AI, massive communicators, service quality, and approach hotspot calamity environment. However, the main challenge is to develop robust applications that support IoT devices in UAV networks with the credibility of a protocols mechanism [11]. The process-controlled system in UAVs has been well developed, but still there are difficulties to manage the flight control system intelligently and under the umbrella of cyber security [12]. There are three ways to enhance the UAV ability of IoT that intelligently solve autonomous flight tasks: (1) flight with single-element intelligence, (2) integrate multi-element intelligence, and (3) autonomous intelligence of UAV Networks [4]. Also needed, with the help of artificial intelligence, is the solving of the network problems of having stationary and mobile nodes in wireless communication in societies [13].

In future, ITS systems and road safety systems will be interrelated with a diversity of systems, like UAVs, vehicles, IoT, and road edge substructure, in order to share more delicate information about UAVs buyers and users of these systems, for example, tracking machine location and speed statistics can be created or infiltrated with malicious objectives. UAVs' communication can be connected to malware security attacks. Those attacks may be on sensitive ITS systems or road safety data. Hence such delicate data needs to be properly defended against autonomous attacks, whose detection must be assured [6]. Figure 12.1 illustrates the modern applications of UAVs.

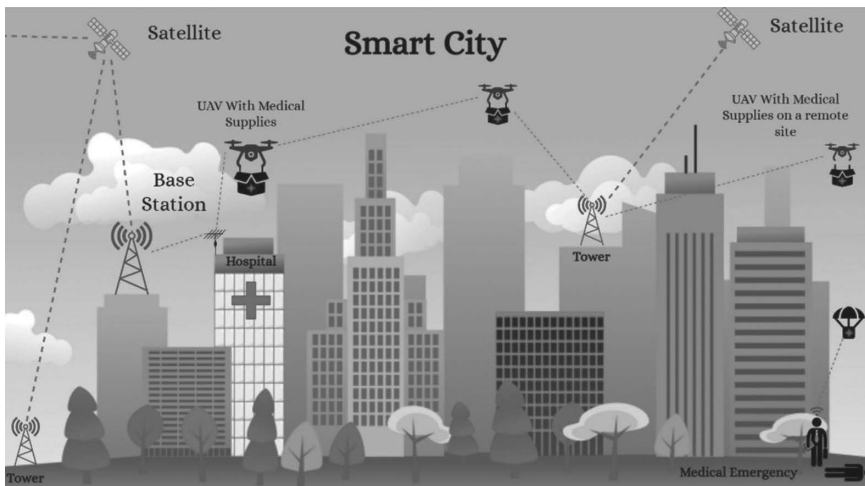


FIGURE 12.1 Applications of UAVs,

12.2 LITERATURE STUDY

In the upcoming decade, revolutionary technologies will be upgraded with 6G technology through international communication equipment (ICT). Everything is adapted to a system that will be intelligent and deeply merged with other devices with the help of a mutual learning process. Artificial intelligence is the key to that kind of process so that communication becomes more inclusive [14].

Among the emerging technologies in the paradigm the Internet of Things (IoT), UAVs show a dominant role [15, 16]. The concurrent technology, IoT, connects with several wireless smart devices. Data is exchanged over 6G communicators via an intelligent transportation system among devices. In this scenario, UAVs play the role of aerial node stations with the IoT infrastructure [13]. Thus trajectory UAVs sync with their mobile sensors nodes (MSN) for transmitting data [17]. In this way, the UAV collects some data through performance indicators for sensing, controlling, and localization based on real-time mobile aerial nodes. Thus they collect some data and send it again to a particular location device if the device moves from its final destination. There they can retransmit data later to the particular device, which is admirable [16]. UAVs routinely work as a mobile relay, pinpointing collected information and updating target sensors for the collected information. They detect signal information by deploying RSSI (received signal strength indication) omnidirectional sensors on UAVs [13].

Prior techniques for improving localization approaches, such as game theory, data fusion, and cooperative localization, are popular in academia [18]. After obtaining the result of the experiment measured with the tracing algorithm in which a group of UAVs is connected to mobile sensors and an unspecified location, only the RSSI of the UAV is used to increase and decrease the signal strength to locate the target. It will depend on the entire knowledge of neighborhood sensor nodes [19]. This method had been used in realistic scenarios. Therefore, on the agenda are high-speed communication with low power consumption, low latency ratio, and security issues that can be dealt with by using protocols. For this purpose, their protocols need to be upgraded over time. Three types of protocols are used in UAV networks [20]:

1. Proactive protocol
2. Reactive protocols
3. Hybrid protocols

Table 12.1 describes the limitations of intelligent transportation systems.

12.3 IOT-ENABLED UAV NETWORKS

Over the last decade, IoT methodology has been developed and is flourishing with the endorsement of UAV network, which has the outstanding technological benefit of managing everything by online command. Meanwhile, the issue of security is important to bear in mind. One of the core security questions is determining which kind of informative data you may need to protect. For example, UAV networks

TABLE 12.1
Limitations of Various Intelligent Transportation Systems

Reference	Technique Used	Description	Limitations
[21]	Self-organizing map (SOM), distributed artificial intelligence (DAI)	This work proposed a novel way to implement DAI and SOM to the transportation system with an energy-efficient operation objective.	DAI needs excessive data to be collected which causes network overloading.
[22]	Earliest deadline first (EDF)	This paper suggested the used of EDF dynamic scheduling algorithm for the melioration of controller area network (CAN) communication network to improve the data transmission rate.	Priority inversion and complexity of this model need to be addressed.
[23]	Artificial neural network (ANN), genetic algorithm (GA), fuzzy logic (FL), expert systems (ES)	This work presented a comparative analysis of artificial analysis techniques for an enhanced intelligent transportation system and concluded ANN is a better approach to implement.	ANN requires great computational power.
[24]	BHTE, federated deep learning (FDL)	This work proposed blockchain-based hierarchical trust evaluation method, BHTE for the intelligent 5G-enabled transport system that deploys DL algorithms with higher system throughput and lower latency.	FDL has high risk of vulnerability to cyber threats, especially data poisoning attacks.
[25]	Residual convolutional neural network (ResNet)	This paper proposed deep learning approach, ResNet for the intelligent detection of the abnormalities on the on-road condition for autonomous vehicle operation to reduce the risk of accidents,	In the ResNet technique, the error detection becomes a grind. Moreover, it shows inefficient learning in some scenarios.

easily locate public transport information and other consumer devices, client special devices, or some common kernel devices that require protection [16].

In the late 1990s, inventors attained a productive usage of the global-positioning system (GPS) in wireless receivers and transceivers (WLAN) as a medium of vehicular communication with the storage of data. The major aims of these actions are to enlarge the road and transportation security and to deflect the impact of malicious

attacks [26]. A big opportunity exists to leak information, which is reason enough to create a war-type situation. UAVs can be used either as reconnaissance vehicles or as lethal weapons. And the reason is that research workers need to protect their sensitive data by providing a web of cyber security [27].

12.4 INTELLIGENT TRANSPORTATION SYSTEM SECURITY ATTACKS

In recent years, due to a pandemic crisis, online jobs provided the best alternatives to meet the needs of the public, cooperators, or employees through remotely delivered services, requiring the exchange of large amounts of data. This had a significant impact on industries such as online marketing, banking, and trading and involved big data. Due to this, the entire world looks like a global village, everything connected through smartphones and IoT devices. Figure 12.2 demonstrates a modern intelligent UAV network.

The exchange of large data increases the risk of malicious threats and security attacks. One such incident happened in 2017, with the famous Petya malware wreaking havoc on Ukrainian organizations, banks, and grids. In the same year, after one more cruel attack by computers of window operating systems (WOS), a rescue base system was clearly needed.

After surveying, more than 50 GB of data had been collected by 2022. However, the security system to protect the required data of each person needed to be

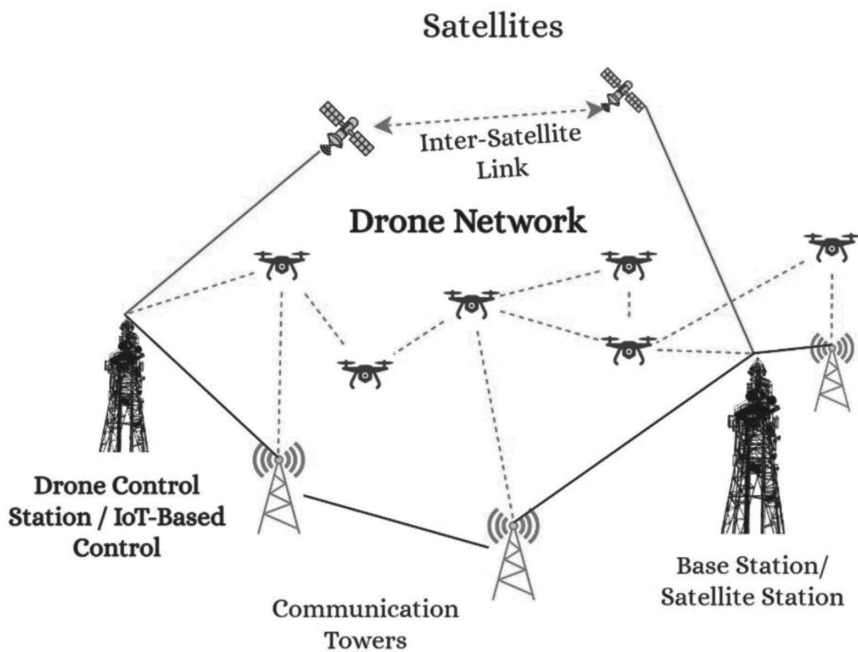


FIGURE 12.2 Intelligent UAV network.

deployed, as a shield against malicious active and passive attacks [28]. This is a snapshot view of the security background system, yet more than five developed countries are working on the 6G network. They have developed smart cities by managing the traffic control systems via ad hoc networks. A bunch of devices used in ad hoc networks are used for navigation fields that go forward to their potential manners. In the previous two decades, the literature has proposed the adoption of more encryption and security systems in flying ad-hoc networks (FANET). This led to work emerging with vehicles ad-hoc (VANET), and mobile ad-hoc networks (MANET) technology [29] to control a big network like a cloud network. This has provided the security of protection against attackers for citizen and military data. There are different types of security attacks on intelligent traffic systems in a UAV smart city, as discussed next.

12.4.1 SHIP AD HOC NETWORK DENIAL OF SERVICE ATTACK

In a ship ad hoc network (SANET), the traffic control system intelligently works among a group of ships, where data was collected by utilizing the appropriate services of IoT-based UAV networks. The first thing is to involve the ship architecture model, which shows a major role in support of the UAV network. Beyond that, the local model of SANET depends on a data collection, data cluster, and localization model. Geographic node coordinates represent the localization data, and every node coordinates different types of data like measuring noise, position data, sea depth, temperature, and wind speed and direction [30]. Moreover, SANET communicates over very high frequency (VHF) to integrate with UAV networks. Networks work in the form of cloud, ad hoc, or swarm network systems and also link with a base station or UAV [31].

When a substantial quantity of data is connected between IoT devices and the UAV system, peer-to-peer security challenges are also there. Often there is a heightened risk of a malicious attack when the network has broken down. Hackers strive to agitate the net cloud, and these types of sudden attacks—such as replay attacks, false data injection (FDI), and denial of service (DoS) attacks—can leave a very horrible impact. The security of the entire network is a very demanding task in a real multi-agent system scenario, requiring security reasoning and intervention of the detection system implemented with the help of significant routing protocols. In the literature, various types of secure control protocols are reported for multi-agent system environments [32].

Denial of service attack, injected via radio interference signal, badly harms systems in a minimum interval of time. Due to this, all multi-agent systems are disconnected from an incident at the time of brutal DoS attacks attack by one individual. Hijackers aim to disconnect all communication lines that are connected with timelines control. As a result, when the ship lost real-time control of direction and speed, it will be lost. It is more difficult to learn the ship tracking control underneath DoS attacks. However, to consider the significance of resource deployment, communication intervals must be designed properly for leveraging the communication load. Therefore, planning in the transmission intervals is one of the keys to suitably designing event-triggering tactics. So the performance could be rigid in a SANET

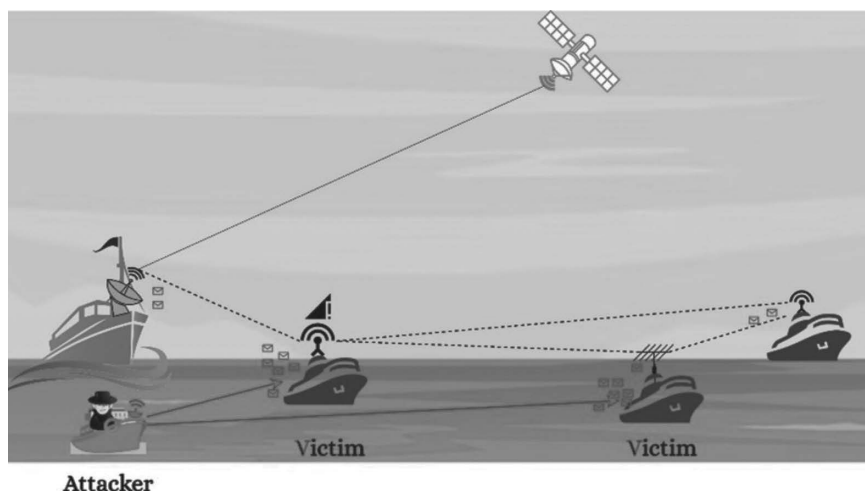


FIGURE 12.3 DoS attack on ship ad hoc network.

system under DoS attacks [33]. Figure 12.3 illustrates the concept of a DoS attack on a SANET.

Particularly, reports have been concerned with establishing control tactics in order to turn into closed-loop systems, which show rigid behavior against DoS attacks, impeding the communication of sensor capacity.

12.4.2 ROBOT AD HOC NETWORK DISTRIBUTED DENIAL OF SERVICE ATTACK

In approximately the last four decades, machinery has taken advantage of rising computational power with new terminology, and robotics has become the most intelligent, vigorous, and enthusiastic type of machinery, consuming less power energy. Moreover, robotics has utilized its alleged ability and has done its work in a form of a network cloud. It means that it has acquired the ability to construct and execute cooperative works. One key of energetic force is the improvement of mutually robot ad hoc systems. This potentially precludes human involvement and responsibilities, which could be made possible by built-in mechanism systems in the robots [34]. Figure 12.4 explains the DDoS attack on a robot ad hoc network in which different clusters are attacking on one another.

Robot ad hoc network (RANET) etiquettes/protocols had been generally studied in terms of two network etiquette: proactive and reactive etiquettes networks. Proactive protocols work in a very small area network, and reactive protocols work in a large network methodology [35]. Both coexisting operating systems work under the subnet, whereas only the proactive type runs between the subnet. The robot ad hoc network works like MANET have the same terminology but with a different name. These terminologies work autonomously in group in UAVs and comprise a robust communication network.

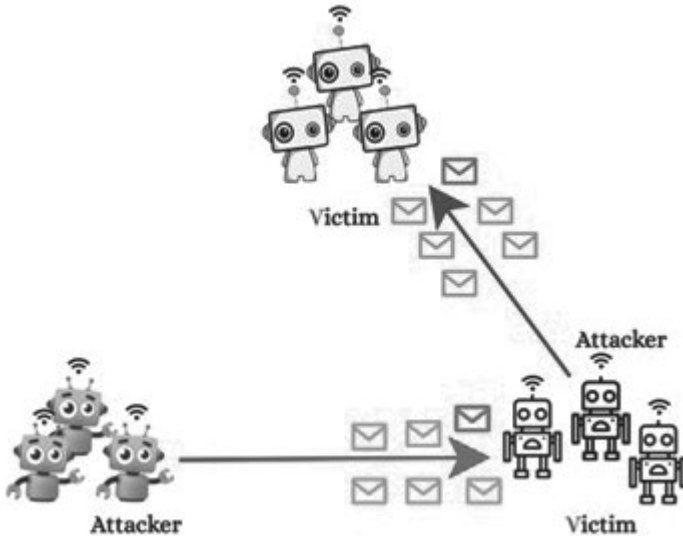


FIGURE 12.4 DDoS attack on a robot ad hoc network.

All technologies have some security threats from attackers. When the technology is spread and works as a multi-agent network system, the security level becomes more challenging. Currently, many security challenges are part of researchers' attention. Although the utmost of cruel threat attacks occur in all fields of RANET, there is also some terminology to prevent serious attacks [36].

1. "Flood" attempts in a network make it difficult to access legitimate network traffic.
2. Try to create a blockage to access service providers.
3. Try to interrupt services and communication between two machines.

The nutshell of all such scenarios is to create a gap between the information of the sender data and information of the receiver data, and prevention of that is a big deal. Another thing is that, in all types of attacks on this type of network, the agent's program has to hold on to the (RANET) network, in which the main system computer is being hunted by using a host computer. Accessing the main computer makes it easy to enter in whole system network with malicious data and control the main system computer with sub-computers [37].

Researchers have emphasized research to fully prevent (DDoS) attacks, but nothing other than adopting numerous defending strategies in a network and neighboring networks has been devised to provide security. Five strategy to secure networks in robotics have been reported [20]:

1. Filtering routers
2. Disabling IP broadcasts

3. Applying security patches
- i4. Disabling unused services
5. Performing intrusion detection

12.4.3 FLYING AD HOC NETWORK THIRD-PARTY ATTACK

The flying ad hoc network is the well-known concept of aircraft autopilot, and it is the most familiar in ITS in machine learning and software-defined networks (SDN). Wireless vision-based sensors are deployed in the services of self-controlled flying vehicles. The mechanism and services are the state-of-the-art intelligent service for flying drones. It connects with a base station or a satellite in multi-UAV systems. Today’s FANET is connected to others in different ways like MANET, VANET, SANET, etc., each having a slightly different mechanism [38].

In this perspective, the ITS has enabled IoT-based UAV single- and multi-agent devices; after the implementation of new devices, the priority is to save human life and secure data. So what are the criteria for precautions to protect it from the hijack? [39]. Third-party attacks and DoSs work in the same way; this means, then, that two nodes are communicating through each other, and the third node behaves like the other two and, being interrupted, sends a fake data packet [20]. Figure 12.5 shows the third-party attack on a FANET.

When a drone is on duty and contains sensitive data, of first importance is its architecture, which keeps it secure by its design and prevents it from becoming a victim. In U2U communication, drones have heuristic drone-based machinery. Computational methods are utilized for threat-sensitive security systems and intrusion detection systems. Significant types of techniques are employed to secure the drone from third-party attacks: cluster (CL), prediction routing network (PR), hierarchal (HR), discovery progress (DP), secure (SR), static (STA), and broadcast [40]. Those methodologies are used to protect against third-party attackers.

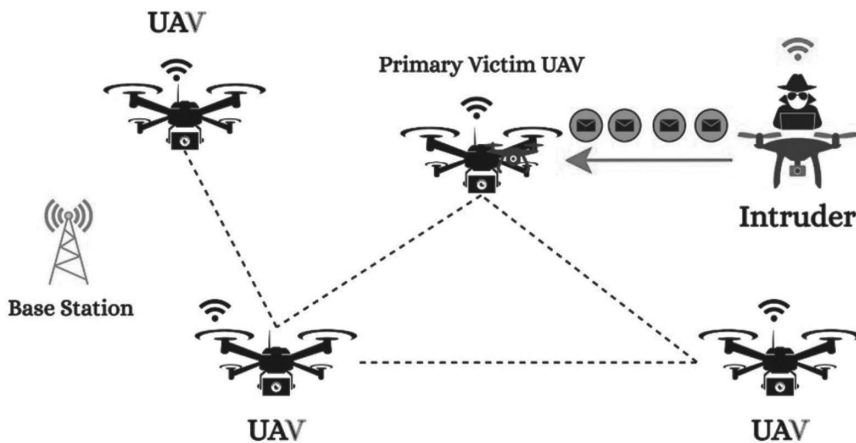


FIGURE 12.5 Third-party attack on FANET.

12.4.4 VEHICULAR AD HOC NETWORK ROUTING ATTACK

Wireless vehicles have been in captivity in this field since the 1980s. In recent years, the authors have witnessed cities being modernized and developed to become big societies; lots of technology goes on behind the scenes. In the field of VANET networks, the research enables a convenient source of services for drivers and passengers. They introduce a new way of transport that is vehicle to vehicle or vehicle to wireless communication infrastructure systems.

However, VANETs work on the basis of direct communication between vehicle and roadside units (RDUs) and easily send and receive information signals on the current timeline. The term “VANET” demonstrates dynamic ad hoc networks, including transportation efficiency applications, green light optimal speed advisory, analyzing and improving route guidance and navigation, lane merging assistants, and car to car communication consortium (C2C-CC). Particularly, the C2C-CC application significantly emphasizes security so that trustworthy information is obtained and protects their ownership. In the past few years, a glance at the literature reveals many broadcast protocols with significant trade-offs. Generally, there are two main classes: multi-hop and single-hop broadcasting data.

Multi-hop broadcasting is a methodology of packet propagation working in a way similar to flooding. For example, when a vehicle source transmits any information in the form of a packet, this packet travels by the nodes of another neighborhood vehicle, re-performs to the next relay vehicle, and, through the same process, further rebroadcasts the same packet until it reaches the final destination vehicle.

On the other hand, in single-hop broadcasting, vehicles do not flood the information packets. Instead, when a vehicle receives a packet from a single hop of broadcasting, it keeps this information to itself on the database board. Occasionally, all vehicles select some sort of record data in their database storage board. The second broadcast information is received in the next cycle. Ultimately, the previous information is transferred to the next neighborhood in one hop. In this way, broadcasting relies on vehicle mobility for spreading information [41].

In both cases, the information is collected by broadcasting. The important thing is how to maintain special and authentic information without any uncertainty or security issues.

After studying various works in the literature, analyzed that record prevalence studies primarily concentrate on efficient strategies that maintain routing etiquettes in VANETs. This approach is mainly based on cryptography and on key management schemes to prevent malevolent nodes from linking to the network. In addition, the major disadvantage of these methods is that they are very profound and expensive, so, given these characteristics of VANETs, using these schemes in the material world is actually problematic.

Numerous vital safety measures are required in VANETs:

1. **Authentication:** In VANET, it is necessary for the sender to endorse a message in order to prevent impersonation.
2. **Concealment:** The privacy and security of every individual must be sheltered. Directional antennas and encrypted data must assure confidentiality.

3. **Integrity:** The integrity of all communications must be separated so that the entrants can modify the content of the message, ensuring that the information is correct.
4. **Non-repudiation:** At the same time, we need to identify attackers after the event is over to prevent hackers from denying the crime.
5. **Availability:** Network resources have to be provided to authentic users but not to the attack ad hoc entities without affecting a network's performance. Some of the routing attacks are [42]:
 - Denial of service (DoS) attack
 - Black hole attack
 - Wormhole attack
 - Sinkhole attack
 - Illusion attack
 - Sybil attack

12.4.5 INTERNET OF THINGS SPOOFING ATTACK

The Internet of Things was created in 1998 by Kevin Ashton. He claimed that an IoT computer is good for communication without human interference. He collected data from things that are connected to wireless devices in terms of smart devices like smart watches, smart appliances, and smart cities. Moreover, IoT devices in smart cities utilize the clouding network, which may start a new epoch of challenges in Internet networking, such as big data interconnected with clouds to organize and manage the city hub. A big network faces many malicious attacks in different scenarios, such as network attacks, distributed denial attacks, spoofing, intrusion detection systems, flood attacks, etc., as discussed in the literature [43].

Providing good network service calls for secure communication, without which attackers can attack systems and, for example, steal confidential information during remote surgery, perhaps leading the patient's death. A spoofed attack works with the electromagnetic wave spectrum and is directly concerned with hackers and military action. It is an illegal activity and may be responsible for starting information warfare (IW). A spoof provides a manipulated GNSS signal data attack on the receiver end; as a result, the signal is altered in velocity and real-time intervals on the receiving side [44].

The spoofing objective may be to eliminate navigation reliability in a confidential area, for example, to falsify the supposed location of the receiver. In this case, the receiver developer would detect this spoofing attack and transmit a counterattack to maintain navigational ability and reliability. A great amount of the literature is focused on anti-spoofing methods [45], and the discussion identifies two different methods of detecting spoofing attacks: routing-based methods and non-routing-based methods.

In the routing method, spoofing packets are entered into the signal network. In this way, the prefix is entered in a filter on the network signal. Routers use ternary content addressable memory (TCAM) to find IP reports to route sachets quickly, but TCAM has limited memory space, which increases the robustness of routers and ultimately signal flow, thus speeding delivery. In addition, TCAM and CAM are

high-power distribution sources and make it pricey in the current trend of network devices; the disadvantage of storing is that flooded inputs are insufficient to store data [46].

The non-routing method introduces the active and passive detection of spoofed traffic. Consequently, in both the active and passive cases, the sender sends data via Internet control message protocol (ICMP) packets from a hostile source, locates the addresses, and receives data from a time-to-line (TTL) traffic network in order to detect incomparable source addresses [47].

In another filtering-based autonomous solution (FaAS), a client has permission to use the network on a contract basis. In this FaAS filter product, authors deploy probed tests for filtering and dropping the spoofing packets, working independently. The probed system generates a minimum number of spoofing packets and discriminates them from the attacker spoofing packet samples [48].

12.4.6 SMART CITIES DATA POISONING ATTACK

The urban population has developed a problem that gets a lot of attention. In the previous ten years, cities have converted into megasocieties and megacities. Cities are not only a hub of human activities but also promise luxurious lifestyles economically, socially, and technologically. Cities have turned into more digitalized, data-based structures that have changed their fundamental environmental needs. The principles, conveyance, economic needs, and other necessary aspects mesh closely with IoT. Also, the invention of the cloud computing network enables the remote control of physical things. A smart city represents a ubiquitous data vitalization process by using top-level applications. Through mobile apps, users can easily access all of the IoT and control things anywhere at any time. The IoT emerged from the evolution of square networks connecting billions of connected devices. Technologies such as ubiquitous computing (UC), wireless sensor networks (WSN), and machine to machine (M2M) are advancing rapidly.

A real smart city comprises big data, complex methodology, information storage, and artificial intelligence abilities. On the other hand, storing large amounts of data is a huge challenge because data networks are diverse. Data collection methods and techniques are closely related to data type and context. Smart cities consist of a wide range of data generated by various city operations, including smart grids, smart buildings, environmental sensors, personal health monitoring, epidemic management, municipal waste management, and disaster management. The main challenge is to store massive data [49].

However, another key that gets the attention of practitioners is the cyber security and privacy of smart grid citizens. The important thing is how to strongly secure all this. Security and privacy are not only linked to basic human rights but are the responsibility of smart grid governance as part of the right of citizenship in a smart city [50]. To resolve this cyber security issue, the first priority is to have a proper strategy against data attacks (DTA). If the data attacker attacks power grid station, the attack on meters is remedied by with fundamental limits of meter measurement strategies, which are intended to work aggressively. In the meantime,

the governors of the grid station may detect the malicious data attacks and react to the interruption [51].

In brief, the route of attacks on smart cities is very different from communication networks compared to the Internet. An attacker’s goal is not only to obtain illegal information but to hold on to smart area hub stations. Most such attacks are on energy management systems (EMSs). In this case, the attacks receive information from external meters, which can be used within a few minutes to immobilize the power grid and revise estimations of the system state. An attacker that can hold the power grid stations can create false meter data to the grid EMS meter. This action confuses the EMS of the control center, which makes faulty decisions regarding the analysis, transmission, or calculation of incidents.

Poison data injection is another way to attack a system. In this method, attackers must have information about the system configuration topology of the smart grid. These configuration settings change systematically, and, in these cases, the attacker won’t have information about the system configuration settings. All information normally is kept secret and under the observation of control-center-regulated authorities [52].

The main benefit of studying the poisoning data attacks is to interpret the weakness that exist in regulations and techniques. The precise impact of such hacks makes clear the system errors and the flaws of measuring data error rate. Figure 12.6 plots the idea of data poisoning attack on smart cities.



FIGURE 12.6 Data poisoning attack on smart cities.

12.5 PRIVACY AND MANAGEMENT IN THE INTELLIGENT TRANSPORTATION SYSTEMS

The intelligent transportation system works dynamically in nonlinear sophisticated systems. In such types of networks, they depend on a source of information, which is provided on a real timeline. Multi-agent cooperators work in ad-hoc-based networks, which may misdirect the information related to the task and put ITS management and privacy at risk [53].

Attackers could pretend to be the authorized supervision and falsify confidential information. These malicious acts can enable attackers to easily access top-secret records internally and externally locate. An external attacker may constantly control the connection and examine all traffic information, but the information cannot be interpreted. On the other hand, internal attackers, such as malicious team agents or employees, have full authority to control public and private information of transportation networks. Consequently, if governors showed compromised behavior, they can become strong attackers. The following attack scenarios were a part of the study [55]:

1. **Impersonation of Genuine Staff:** The attacker appears to be a staff member and accesses confidential information.
2. **Malicious Staff:** Malicious actions can lead to unauthorized access to information and serious emergencies.
3. **Greedy Staff:** Greedy staff takes advantage of their privilege and generate needless trouble such as traffic jams, lane blocking, etc.

For that reason, intelligent privacy and security technologies are needed to obfuscate things for attackers, or strategies are needed to find these connected entities. These steps are necessary to detect malicious content. Significantly, researchers have been working on how to achieve privacy using public key infrastructure (PKI) [56]. Two types of encryption rules allow the implementation of privacy-aware policies.

1. **Policy-Based Encryption:** This cryptographic primitive needs data for encryption regarding policies.
2. **Policy-Based Signature:** These cryptographic primitives create digital signatures based on policies agreed upon between establishments. These cryptographic benefits include privacy policy creation, automatic trust negotiation, trust generation, access control, etc. [57].

12.6 DATA MANAGEMENT IN THE INTELLIGENT TRANSPORTATION SYSTEM

Data is the backbone of many production and whole system organizations. The capability of smart tools and strategies to capture and participate in environmental measurements as data leads to the creation of smart services for the benefit of people [58]. Data management is state-of-the-art work; all elements are involved from

architecture to data quality. Every network has some limitations, and every network has some advantages based on trade-offs factors.

Data management aims to enable data to be shared, editable, and stored, with the characteristics of quality and performance and with appropriate sensors and detectors. The capability to achieve data quality is directly concerned with user archive data attributes in the ITS: data accuracy, falsified data, missed data, and, in some cases, data retrieval collection [59]. The enrollment of data management in intelligent transportation systems (ITS) requires conveniently monitoring the traffic data management operators and retaining it in a systematic way by archived data user services. The main challenge concerns the irregularity of swapped information. This challenge is normally created by an error of sensors, failures, bad web net, and GPS net handling.

Comparably confusing data deliberately circulates in our society. The big challenge is to chasing down this type of data, like fraud, false data, randomly generated data without sensors, gain revenue/credits for sharing falsified data. The main aim is achieving the identification of strange and trustworthy crowd-sourced information, in the meantime staying focused on the growing mobility services of data between users [60].

12.7 BLOCKCHAIN-BASED INTRUSION DETECTION SYSTEM FOR THE INTELLIGENT TRANSPORTATION SYSTEM

The key factors of security, privacy, and trustworthy environment in ITS infrastructure are a widely critical issue. Every person has a vehicle requirement. With the ITS in transportation sector, security is a more critical problem for users and authorities.

At the present time, smart/intelligent transportation systems cooperate with blockchain technology and with intrusion detection system. In intrusion detection systems, the intrusion security systems alert the concerned person before the attack happens.

Normally, intrusion detection systems are described in two classes:

2. **Network Intrusion Detection System (NIDS):** Close supervision and registration will allow this network to work freely with all the gadgets and other devices.
2. **Host Intrusion Detection System (HIDS):** In this way, only one computer works as a host, which manages and controls the monitoring of traffic flow data packets and leads work to safe malicious attack data [61].

Blockchain is a digitalized system network that works in a way similar to that of distributed levels. It is mostly applicable in accounts, banking, and ledger for transaction data. It cannot work on a signal entity or node but rather works on the basis of cluster grouping and arrays. Working on logical consensus, it takes decisions with the help of previously stored data in the form of arrays. After checking those arrays, it generates opinions automatically in regular intervals on every transaction. In today's lifestyle, blockchain works efficiently in our daily tasks such as in cryptocurrency, bitcoin, intrusion detection (cyber security), automation, modex application, etc. [62].

Blockchain with structural architecture in ITS network has a variety of advantages [63]:

1. No single entity is swapping or dealing with isolated transaction ledgers, or there is a single failure in the network.
2. Each group has equal rights because it has no power. Each group has equal rights because there is no opportunity for dirty ownership power.
3. Thanks to the blockchain system, fraud and falsification can be avoided.

12.8 ARTIFICIAL-INTELLIGENCE-BASED SECURITY MECHANISM FOR UNMANNED AERIAL VEHICLES

In unmanned aerial vehicle (UAV) communication, the collection of data sent and received is the key factor in this technology. Through this type of network, a massive situational awareness in emergency response, disaster management, and security processes are enabled by using pattern recognition approaches [64]. Most of the time, they provide lots of data where there is security risk in, say, a dark area or away from any eyewitness; camera sensors can recognize an incident. For example, road accidents can be minimized by UAV-2-UAVs. UAVs are resource control device communication systems that minimize sudden mishap accidents [65].

On the other hand, security is an issue of its own in UAVs. Due to its wireless medium, it handles all information in intervals. In the literature, two types of security mechanisms to protect the networks are discussed: cryptography and the intrusion detection system [66]. The basis of research in the expansion of UAVs is the expansion of control systems. At the current state of development, the problem of automatic flight control has been solved, but the problem of regulatory intelligent safety mechanisms has not been fully cracked [67]. In the security mechanism, the encryption process can be implemented on all devices that are connected to UAVs. Flight control, MANET, and ad hoc networks can be processed by their hardware mechanism as well as by their software mechanism, and the security mission is provided by the control system [68].

One study has led to the invention of security mechanisms based on artificial-intelligence-based communication and classification for UAVs: the Effective Emergency Monitoring System (AISCC-DE2MS):

1. AISCC-DE2MS performance uses the artificial gorilla unity optimizer (AGTO) algorithm with ECC-based El Gamal encryption technology to provide security mechanisms.
2. The AISCC-DE2MS model for instant-based state arrangement features dense net network feature extraction (dense net), penguin search optimization (PESO)-based hyperparameter tuning, and instant-based classification, long short-term memory (LSTM).

Simulation analysis of the AISCC-DE2MS model is performed using the AIDER database.

12.9 FUTURE DIRECTIONS

Security encryption is a growing issue in the future with developing IoT and UAV technologies. Most of the security work on denial attacks in the past decades has been on distributed denial attacks encrypted by various protocols, but there is some elasticity in security protocols privilege, and stringent laws are needed for the communication network to be right. For this aim, the future direction of GA and its evolutionary computational techniques, swarm optimization, machine learning, and deep learning can be employed with sensor devices in arbitrary situations to evaluate optimal encryption [69]. Other research calls attentions to the need for significant progress in the security of UAVs, which might be best resolved by AI and ML from malware attacks [70]. Deebak et al. [71] demonstrate performance in their research work based on drones and lightweight UAVs. Privacy preserving schemes have been noted in discrete communication IoTs with enhancement with Python/C++ protocols. Even though other numerous works must be focused on in future, such as gateway trajectory and UAV protocols, key management and authentication are more properly investigated and promise innovative solutions with restricted specific limitations and requirements [72].

12.10 CONCLUSION

The security issue of modern inventions revolves around us in different ways. The authors used coined methodology to optimize big issues. In that respect, many reporters report varieties of tools and tactics in the form of protocols and algorithms. A few authors suggest that changes built into their system design architecture could be taken advantage of for attack protection. These changes could be easily implemented in devices. Furthermore, IoT-based devices have intelligent transportation systems that minimize human responsibility and that provide error-free data in real time. This chapter presented a comprehensive overview in detail of various security threats and limitation, with the emphasis more on security and privacy management and on simulations and evolutionary techniques to fill this gap.

REFERENCES

- [1] Kashif Qureshi, Hanan Abdullah, "A survey on intelligent transportation systems," *Middle-East Journal of Scientific Research*, vol. 15, no. 5, pp. 629–642, 2013.
- [2] Min Sheng, Nan Zhao, Chengwen Xing, Weidang Lu, Xianbin Wang, Xu Jiang, "Green UAV communications for 6G: A survey," *Chinese Journal of Aeronautics*, vol. 35, no. 9, pp. 19–34, Sep 2022.
- [3] Mohamed-Amine Lahmeri, Mustafa A. Kishk, Mohamed-Slim Alouini, "Artificial intelligence for UAV-enabled wireless networks: A survey," *IEEE Open Journal of the Communications Society*, vol. 23, no. 2, pp. 1015–1040, Apr 2021.
- [4] Rui Yin, Wei Li, Zhi-qiang Wang, Xin-xin Xu, "The application of artificial intelligence technology in UAV," in *2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)*, IEEE, pp. 238–241, Nov 2020.
- [5] Sifat Rezwan, Wooyeol Choi, "Artificial intelligence approaches for UAV navigation: Recent advances and future challenges," *IEEE Access*, vol. 8, Mar 2022.

- [6] Hamid Menouar, Ismail Guvenc, Kemal Akkaya, A. Selcuk Uluagac, Abdullah Kadri, Adem Tuncer, "UAV-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, Mar 2017.
- [7] Inam Ullah Khan, Ijaz Mansoor Qureshi, Muhammad Adnan Aziz, Tanweer Ahmad Cheema, Syed Bilal Hussain Shah, "Smart IoT control-based nature inspired energy efficient routing protocol for flying ad hoc network (FANET)," *IEEE Access*, vol. 8, pp. 56371–56378, Mar 2020.
- [8] Muhammad Asghar Khan, Alamgir Safi, Ijaz Mansoor Qureshi, Inam Ullah Khan, "Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols," in *2017 First International Conference on Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT)*, IEEE, pp. 1–9, Nov 2017.
- [9] Saeed Hamood Alsamhi, Alexey V. Shvetsov, Santosh Kumar, Jahan Hassan, Mohammed A. Alhartomi, Svetlana V. Shvetsova, Radhya Sahal, Ammar Hawbani, "Computing in the sky: A survey on intelligent ubiquitous computing for UAV-assisted 6g networks and industry 4.0/5.0," *Drones*, vol. 6, no. 7, p. 177, Jul 2022.
- [10] Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, Dapeng Oliver Wu, "Edge computing in industrial internet of things: Architecture, advances and challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, Jul 2020.
- [11] Arafatur Rahman, A. Taufiq Asyhari, "The emergence of internet of things (IoT): Connecting anything, anywhere," *Computers*, vol. 8, no. 2, p. 40, May 2019.
- [12] Jason Whelan, Abdulaziz Almeahmadi, Khalil El-Khatib, "Artificial intelligence for intrusion detection systems in unmanned aerial vehicles," *Computers and Electrical Engineering*, vol. 99, p. 107784, Apr 2022.
- [13] Yannis Spyridis, Thomas Lagkas, Panagiotis Sarigiannidis, Vasileios Argyriou, Antonios Sarigiannidis, George Eleftherakis, Jie Zhang, "Towards 6G IoT: Tracing mobile sensor nodes with deep learning clustering in UAV networks," *Sensors*, vol. 21, no. 11, p. 3936, Jun 2021.
- [14] Yang Lu, Xianrong Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues," *Journal of Industrial Information Integration*, vol. 19, p. 100158, Sep 2020.
- [15] Thomas Lagkas, Vasileios Argyriou, Stamatia Bibi, Panagiotis Sarigiannidis, "UAV IoT framework views and challenges: Towards protecting drones as 'Things'," *Sensors*, vol. 18, no. 11, p. 4015, Nov 2018.
- [16] Zhiqiang Xiao, Yong Zeng, "An overview on integrated localization and communication towards 6G," *Science China Information Sciences*, vol. 65, pp. 1–46, Mar 2022.
- [17] Cheng Zhan, Yong Zeng, Rui Zhang, "Energy-efficient data collection in UAV enabled wireless sensor network," *IEEE Wireless Communications Letters*, vol. 7, no. 3, pp. 328–331, Nov 2017.
- [18] Ali Yassin, Youssef Nasser, Mariette Awad, Ahmed Al-Dubai, Ran Liu, Chau Yuen, Ronald Raulefs, Elias Aboutanios, "Recent advances in indoor localization: A survey on theoretical approaches and applications," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1327–1346, Nov 2016.
- [19] Bultitude, Yvo de Jong, Terhi Rautiainen, *IST-4-027756 WINNER II DI. 1.2 VI. 2 WINNER II Channel Models. EBITG, TUI, UOULU, CU/CRC, NOKIA*, Tech. Rep, 2007.
- [20] Khaista Rahman, Muhammad Adnan Aziz, Ahsan Ullah Kashif, Tanweer Ahmad Cheema, "Detection of security attacks using intrusion detection system for UAV

- networks: A survey,” in *Big Data Analytics and Computational Intelligence for Cybersecurity*, Springer International, vol. 2, pp. 109–123, Sep 2022.
- [21] Pratik Goswami, et al., “AI based energy efficient routing protocol for intelligent transportation system,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1670–1679, 2021.
- [22] Zhihan Lv, Ranran Lou, Amit Kumar Singh, “AI empowered communication systems for intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4579–4587, 2020.
- [23] Mirialys Machin, et al., “On the use of artificial intelligence techniques in intelligent transportation systems,” in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, IEEE, 2018.
- [24] Xiaoding Wang, et al., “Heterogeneous blockchain and ai-driven hierarchical trust evaluation for 5G-enabled intelligent transportation systems,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 2, pp. 2074–2083, 2023.
- [25] Rozi Bibi, et al., “Edge AI-based automated detection and classification of road anomalies in VANET using deep learning,” *Computational Intelligence and Neuroscience*, vol. 2021, pp. 1–16, 2021.
- [26] H. Hartenstein, L. P. Laberteaux, “A tutorial survey on vehicular ad hoc networks,” *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, Jun 2008.
- [27] Bisma Baig, Abdul Qahar Shahzad, “Machine learning and AI approach to improve UAV communication and networking,” in *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*, Springer International Publishing, vol. 30, pp. 1–15, Mar 2022.
- [28] Muhammad Hassan, Sher Ali, Muhammad Imad, Shaista Bibi, “New advancements in cybersecurity: A comprehensive survey,” *Big Data Analytics and Computational Intelligence for Cybersecurity*, vol. 2, pp. 3–17, Sep 2022.
- [29] Inam Ullah Khan, Muhammad Abul Hassan, Muhammad Fayaz, Jeonghwan Gwak, Muhammad Adnan Aziz, “Improved sequencing heuristic DSDV protocol using nomadic mobility model for FANETS,” *Computers, Materials and Continua*, vol. 70, no. 2, pp. 3653–3666, Jan 2022.
- [30] Sumaya Hamad, Yossra Hussain Ali, Shaimaa H. Shaker, “Localization technique model of ships ad hoc network (SANET) using geographic’s database and clustering analysis,” *International Journal of Online & Biomedical Engineering*, vol. 18, no. 6, Jun 2022.
- [31] Rabab Al-Zaidi, John Woods, Mohammed Al-Khalidi, Khattab M. Ali Alheeti, Klaus McDonald-Maier, “Next generation marine data networks in an IoT environment,” in *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, IEEE, pp. 50–55, May 2017.
- [32] Wenyong Xu, Guoqiang Hu, Daniel W. C. Ho, Zhi Feng, “Distributed secure cooperative control under denial-of-service attacks from multiple adversaries,” *IEEE Transactions on Cybernetics*, vol. 50, no. 8, pp. 3458–3467, Feb 2019.
- [33] Yang Tang, Dandan Zhang, Daniel W.C. Ho, Wen Yang, Bing Wang, “Event-based tracking control of mobile robot with denial-of-service attacks,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 9, pp. 3300–3310, Nov 2018.
- [34] Zhigang Wang, MengChu Zhou, N. Ansari, “Ad-hoc robot wireless communication,” in *SMC’03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance*, IEEE (Cat. No. 03CH37483), vol. 4, pp. 4045–4050, Oct 2003.
- [35] Zhigang Wang, Lichuan Liu, Mengchu Zhou, “Protocols and applications of ad-hoc robot wireless communication networks: An overview,” *Future*, vol. 10, p. 20, 2005.

- [36] Felix Lau, Stuart Rubin, M.H. Smith, Ljiljana Trajkovic, "Distributed denial of service attacks," in *SMC 2000 Conference Proceedings. 2000 IEEE International Conference on Systems, Man and Cybernetics. Cybernetics Evolving to Systems, Humans, Organizations, and Their Complex*, IEEE, pp. 2275–2280, Oct 2000.
- [37] Shui Yu, *Distributed Denial of Service Attack and Defense*, Springer, 2014.
- [38] İlker Bekmezci, Ozgur Koray Sahingoz, Şamil Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, May 2013.
- [39] Muhammad Abul Hassan, Muhammad Imad, Tayyabah Hassan, Farhat Ullah, "Impact of routing techniques and mobility models on flying ad hoc networks," in *Computational Intelligence for Unmanned Aerial Vehicles Communication Networks*, Springer International, vol. 30, pp. 111–129, Mar 2022.
- [40] Muhammad Asghar Khan, Insaf Ullah, Shibli Nisar, Fazal Noor, Ijaz Mansoor Qureshi, Fahimullah Khanzada, Hizbullah Khattak, Muhammad Adnan Aziz, "Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, vol. 2020, Jul 2020.
- [41] Sooksan Panichpapiboon, Wasan Pattara-Atikom, "A review of information dissemination protocols for vehicular ad hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 3, pp. 784–798, Aug 2011.
- [42] Priyanka Sirola, Amit Joshi, Kamlesh C. Purohit, "An analytical study of routing attacks in vehicular ad-hoc networks (VANETs)," *International Journal of Computer Science Engineering (IJCSSE)*, vol. 3, no. 4, pp. 210–218, Jul 2014.
- [43] J. Rossouw van der Merwe, Xabier Zubizarreta, Ivana Lukčičin, Alexander Rügamer, Wolfgang Felber, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*, Gothenburg, Sweden, pp. 91–99, 2018, doi:10.1109/EURONAV.2018.8433227.
- [44] Mark L. Psiaki, Todd E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, Apr 2016.
- [45] Ali Jafarnia-Jahromi, Ali Broumandan, John Nielsen, Gérard Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.
- [46] Mukrimah Nawir, Amiza Amir, Naimah Yaakob, Ong Bi Lynn, "Internet of things (IoT): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, pp. 321–326, Aug 2016.
- [47] Steven J. Templeton, Karl E. Levitt, "Detecting spoofed packets," in *Proceedings DARPA Information Survivability Conference and Exposition*, IEEE, pp. 164–175, Apr 2003.
- [48] Hamzeh Mohammadnia, Slimane Ben Slimane, "IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network," in *2020 Seventh International Conference on Software Defined Systems (SDS)*, IEEE, pp. 5–13, Apr 2020.
- [49] Bhagya Nathali Silva, Murad Khan, Kijun Han, "Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities," *Sustainable Cities and Society*, vol. 38, pp. 697–713, Apr 2018.
- [50] James Curzon, Abdulaziz Almeahmadi, Khalil El-Khatib, "A survey of privacy enhancing technologies for smart cities," *Pervasive and Mobile Computing*, vol. 55, pp. 76–95, Apr 2019.
- [51] Oliver Kosut, Liyan Jia, Robert J. Thomas, Lang Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–58, Oct 2011.
- [52] Oliver Kosut, Liyan Jia, Robert J. Thomas, Lang Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *2010 First*

- IEEE International Conference on Smart Grid Communications*, IEEE, pp. 220–225, Oct 2010.
- [53] Aneta Zwierko, Zbigniew Kotulski, “Mobile agents: Preserving privacy and anonymity,” *Lecture Notes in Computer Science*, vol. 3490, pp. 246–258, Sep 2005.
- [54] Dalton Hahn, Arslan Munir, Vahid Behzadan, “Security and privacy issues in intelligent transportation systems: Classification and challenges,” *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 181–196, Apr 2019.
- [55] Andrew S. Patrick, Moti Yung, *Financial Cryptography and Data Security*, Springer Berlin Heidelberg, 2005.
- [56] Suresh Chavhan, Deepak Gupta, Sahil Garg, Ashish Khanna, Bong Jun Choi, M. Shamim Hossain, “Privacy and security management in intelligent transportation system,” *IEEE Access*, vol. 8, pp. 148677–148688, Aug 2020.
- [57] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin Shen, Jinshu Su, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, Jun 2010.
- [58] Mirko Zichichi, Stefano Ferretti, Gabriele D’angelo, “A framework based on distributed ledger technologies for data management and services in intelligent transportation systems,” *IEEE Access*, vol. 8, pp. 100384–100402, May 2020.
- [59] Shawn M. Turner, Robert J. Benz, Luke P. Albert, “ITS data archiving: Case study analyses of San Antonio TransGuide data,” *Texas Transportation Institute*, vol. 1, Jan 1999.
- [60] *Mobi: Mobility Open Blockchain Initiative*, 2020 [Online]. Available: <https://dlt.mobi/>.
- [61] A. Mohan Krishna, Amit Kumar Tyagi, “Intrusion detection in intelligent transportation system and its applications using blockchain technology,” in *2020 International Conference on Emerging Trends in Information Technology and Engineering (IC-ETITE)*, IEEE, pp. 1–8, Feb 2020.
- [62] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system Bitcoin,” *Bitcoin.org*, 2009. Disponible en <https://bitcoin.org/en/bitcoin-paper>.
- [63] Yong Yuan, Fei-Yue Wang, “Towards blockchain-based intelligent transportation systems,” in *2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC)*, IEEE, pp. 2663–2668, Nov 2016.
- [64] H. Sedjelmaci, S. M. Senouci, N. Ansari, “A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no 9, pp. 1594–1606, 2017.
- [65] Aicha Idriss Hentati, Lamia Chaari Fourati, “Comprehensive survey of UAVs communication networks,” *Computer Standards & Interfaces*, vol. 72, p. 103451, Oct 2020.
- [66] Hichem Sedjelmaci, Sidi Mohammed Senouci, Nirwan Ansari, “A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1594–1606, Mar 2017.
- [67] Rui Yin, Wei Li, Zhi-qiang Wang, Xin-xin Xu, “The application of artificial intelligence technology in UAV,” in *2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT)*, IEEE, pp. 238–241, Nov 2020.
- [68] Fatma S. Alrayes, Saud S. Alotaibi, Khalid A. Alissa, Mashaal Maashi, Areej Alhogaib, Najm Alotaibi, Heba Mohsen, Abdelwahed Motwakel, “Artificial intelligence-based secure communication and classification for drone-enabled emergency monitoring systems,” *Drones*, vol. 6, no. 9, p. 222, Aug 2022.
- [69] F. Subhan, M. A. Aziz, I. U. Khan, M. Fayaz, M. Wozniak, J. Shafi, M. F. Ijaz, “Cancerous tumor controlled treatment using search heuristic (GA)-based sliding mode and synergetic controller,” *Cancers*, vol. 14, no. 17, p. 4191, 2022.

- [70] Y. Yazid, I. Ez-Zazi, A. Guerrero-González, A. El Oualkadi, M. Arioua, “UAV-enabled mobile edge-computing for IoT based on AI: A comprehensive review,” *Drones*, vol. 5, no. 4, p. 148, 2021.
- [71] B. D. Deebak, F. Al-Turjman, “A smart lightweight privacy preservation scheme for IoT-based UAV communication systems,” *Computer Communications*, vol. 162, pp. 102–117, 2020.
- [72] Hassan Jalil Hadi, et al., “A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs,” *Journal of Network and Computer Applications*, p. 103607, 2023.

13 Cyber Attack Detection Analysis Using Machine Learning for IoT-Based UAV Network

Usman Haider, Hina Shoukat, Muhammad Yaseen Ayub, Muhammad Tehmasib Ali Tashfeen, Tarandeep Kaur Bhatia, and Inam Ullah Khan

13.1 INTRODUCTION

The aerial ad hoc network is a newly emerged technology from MANETs. A-ANETs are used to group UAVs. Due to the involvement of IoT in UAV networks, a novel area of research is introduced, known as the Internet of Drones. UAVs have applications in both the civil and military domains. On the civil side, UAVs are commonly utilized in forestry, disaster management, sports, rescue operations, and smart farming as well. UAVs can be used for the surveillance and detection of intruders [1, 2]. Cellular-connected UAVs are considered the advanced approach that overcomes end-to-end connectivity. Wireless networks like 5G and beyond in UAV networks will improve latency problems [3]. The agricultural industry has been revolutionized with the help of aerial vehicles, which are used to monitor crops more effectively [4]. Secure communication in UAVs is considered a serious problem. Intruders deploy DoS/DDoS security attacks to easily take control of the entire network. The attacker sends malicious data packets continuously to hijack the network. Denial of service is commonly called a third-party attack, which can render a valid workstation unavailable [5]. Domain name system [6], distributed denial of service [7], and Sybil [8] attacks can unbalance high accuracy. However, to identify real and fake attacks in UAV networks, there will be true/false positive and true/false negative approaches. A-ANETs have very short range of communication but are uniquely self-organizing in nature. Due to their dynamic movement, aerial vehicles are more exposed to cyber attacks [9]. Figure 13.1 illustrates the concept of sending fake data packets to UAV networks for jamming or hijacking.

Over-the-Internet identification of various attacks are quite difficult. Different methods and software help users in the detection of cyber attacks. Game theory technique can be used to detect intruders [10]. The intrusion detection system is designed to detect possible security attacks. This chapter offers insightful information about

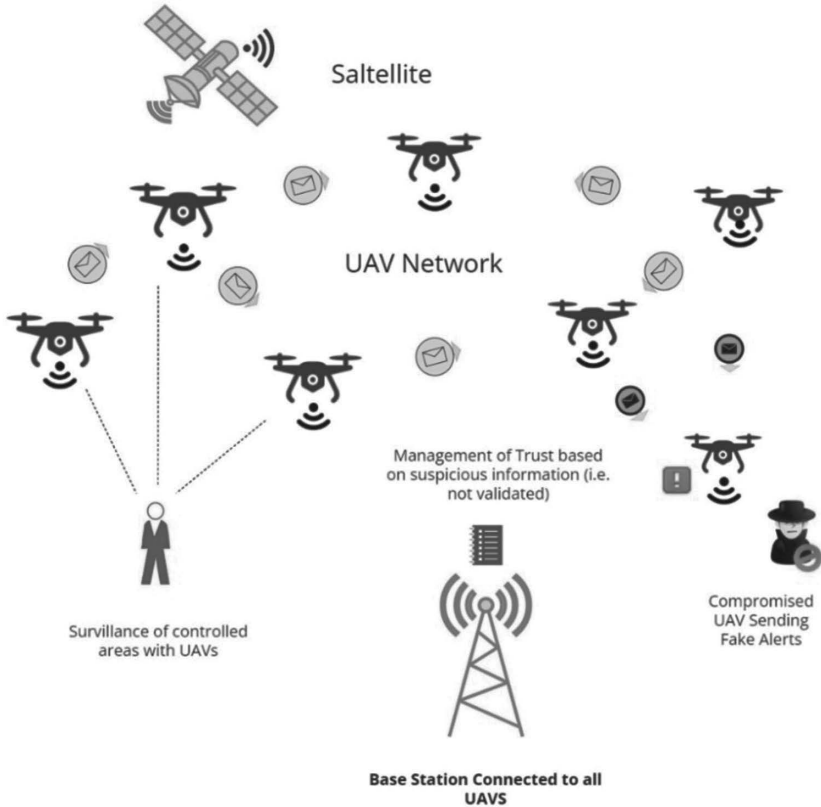


FIGURE 13.1 Scenario of UAV network with fake data packets.

the IDS, like anomaly, signature, and hybrid techniques. Machine learning classifiers use specific datasets to detect attacks easily. Recently, machine learning techniques have been widely utilized to detect attacks. ML algorithms give speedy results in comparison with other techniques [11]. Major contribution points of this research are as follows:

- The IoT-based aerial ad hoc network concept is introduced.
- A detailed comparative study of machine learning techniques like XGBoost, naïve Bayes, complement naïve Bayes, AdaBoost, and GaussianNB are performed using the UNSW-NB 15 dataset.
- Analysis of machine learning based IDS study is incorporated.

13.2 LITERATURE STUDY

This section presents the limitations of machine- and deep-learning-based intrusion detection systems. Also, traditional techniques of the IDS are discussed in

detail. Security is considered one of the major concerns in almost every field of study. Specifically, the intrusion detection system is widely utilized in network traffic analysis to detect possible attacks. Deep learning models are used to learn and train real-time network performance in terms of identifying security attacks [12–14]. In the near future, therefore, personnel will be reduced, and machines, robots, UAVs, and IoT devices will take control. Due to fake and real traffic, data detection will be the main problem. Raw or unwanted data slows down and reduces the computational efficiency of the overall network. Preprocessing data needs to be further explored through machine learning techniques [15–17].

Network-level attack detection is quite useful on autonomous machines. Data sharing is usually formed to connect resources of various nodes. Intermixing various features of different techniques formulates hybrid IDS models that retain advantages over multiple techniques [18, 19]. User behavior can also be either normal or suspected. Therefore, rule-based security expert systems are able to detect fake data. This approach is mostly used for large datasets [20–24].

IoT-based network system data traffic must be monitored to detect possible security attacks. IDS self-protection is quite an unrealistic approach. Therefore, anomaly-based IDS has various issues that include unwanted data detection. Information gain and gain ratio approaches are used to extract optimal features. The NSL-KDD dataset is utilized over machine learning techniques to check performance. Intersection and union methods are helpful over IoT networks [25]. Further, drawbacks of various machine learning techniques are presented in Table 13.1. In addition, various datasets are explained with different fields of studies.

TABLE 13.1
Detailed Study of IDS Using Machine Learning with Limitations

Reference	Field of Study	Type of IDS	Dataset	Limitation of IDS	Description
[26]	IoT	Integrated intrusion-detection (IID) system	DNN	Sometimes IDS is unable to detect cyber attacks.	IID system, independent of IoT protocols and network structure with no prior requirement of knowledge of threats
[27]	IoT	CNN-powered with reptile search algorithm (RSA),	KDDCup-99, NSL-KDD, CICIDS-2017 and BoT-IoT	IDS have a significant false alarm rate.	The system relies on deep learning and metaheuristic (MH) optimization algorithms (i.e., RSA), along with implementation of effective convolutional neural network (CNN) as the core feature.

(Continued)

TABLE 13.1 (Continued)
Detailed Study of IDS Using Machine Learning with Limitations

Reference	Field of Study	Type of IDS	Dataset	Limitation of IDS	Description
[28]	IoT	IDS with hybrid data optimization using RF algorithm	UNSW-NB15	IDS time monitoring is not effective.	This system utilized isolation forest (iForest) and genetic algorithm (GA) to eliminate outliers and to achieve optimal results. Random forest (RF) classifier is used as the evaluation criterion.
[29]	IoT	Suricata IDS/IPS	—	Signature-based IDS is unable to detect zero-day attacks.	The anomaly- and signature-based IDS using hybrid inference systems is deployed, along with the NN model for the metaheuristic’s manual detection of malicious traffic in the targeted network.
[30]	IoT	Anomaly-based IDS for IoT ecosystem	NSL-KDD	IDS only reveals attacks, so external force is needed to prevent them.	Paper proposed an IDS using ML with the feature selection method and showed implementation of the selection and extraction approach with anomaly-based IDS.
[31]	IoT	NIDS through an SDN	NSL-KDD	Susceptible to protocol-based attacks.	Network-monitoring-based machine learning techniques have been applied.
[32]	IoT	Anomaly-based IDS	CSE-CIC-IDS2018-V2’	The anomaly-based IDS has high false alarm rate.	The GBM ensemble is a key feature in this approach applied to train the binary classifier with the application of preprocessed records.

13.3 INTRUSION DETECTION SYSTEM USING MACHINE LEARNING

The intrusion detection system is mostly used to identify security attacks. However, the anomaly-based IDS formulates a threshold to detect unknown attacks. Data traffic monitoring is associated with packet headers. IDS techniques are quite advanced in detecting abnormal behaviors of an intruder. Attacks can be either active or

passive, which destroy overall network infrastructure [33–35]. Further, machine-learning-based techniques are implemented for IDS to detect unknown data packets. IoT networks consist of hardware components, where irrelevant data slow down the entire system. The accuracy of IoT-based networks is reduced, which directly affects data modeling. Flexible mutual information-based feature selection identifies cyber threats using the anomaly-based approach in IoT networks [36–38]. In addition, K -NN, ANN, and bagging are used to rank the features of unknown data in a network. Working on machine learning techniques requires datasets that are helpful in data preprocessing, model training, and testing. NSL-KDD and KDD99 are the datasets that are mostly utilized for experimentation [39].

13.4 PROPOSED SYSTEM MODEL

Figure 13.2 describes the system model, which consists of the UNSWNB-15 dataset. There are two datasets: training and testing. Further, to balance overall dataset

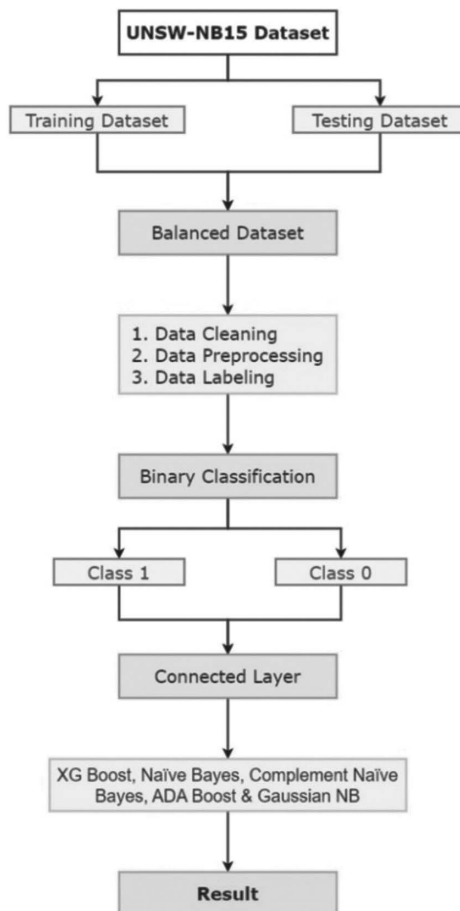


FIGURE 13.2 System model using machine learning techniques.

data cleaning, data preprocessing and labeling are performed. For classification, the binary method is utilized. Machine learning classifiers like XGBoost, naïve Bayes, complement naïve Bayes, AdaBoost, and GaussianNB are used detect accurately cyber attacks from the UNSWNB-15 dataset. The system model dataset needs to be balanced with binary classification. Therefore, classes “0” and “1” is merged with the connected layer. IoT-enabled UAVs are utilized to connect people, data, and things. Cyber attacks are considered one of the critical issues in IoT-enabled UAVs. UNSWNB-15 has around nine different types of attacks: fuzzers, backdoors, denial of service, exploits, generic, reconnaissance, shellcode, worm, and analysis. Class labeling with around 49 features is developed. However, machine-learning-based intrusion detection is a better solution for detecting cyber attacks.

13.5 SIMULATION RESULTS

The simulation environment is made possible using Python. UNSW-NB 15 dataset is utilized where other existing datasets contain old information. UNSW-NB has abnormal data packets, which are quite helpful for IoT-based UAV networks to detect cyber attacks [40–52].

Machine learning algorithms are implemented on training and testing datasets, respectively. Binary classification is performed on the overall simulation of XGBoost, naïve Bayes, complement naïve Bayes, AdaBoost, and GaussianNB. Figure 13.3 shows the normal and abnormal behavior of network traffic. Around 75.99% is normal, and 24.01 % is considered abnormal. Table 13.2 describes the information in Figure 13.4, which has the simulation results of machine learning algorithms like XGBoost, naïve Bayes, complement naïve Bayes, AdaBoost, GaussianNB in terms of accuracy. In overall, results accuracy with XGBoost and AdaBoost performance

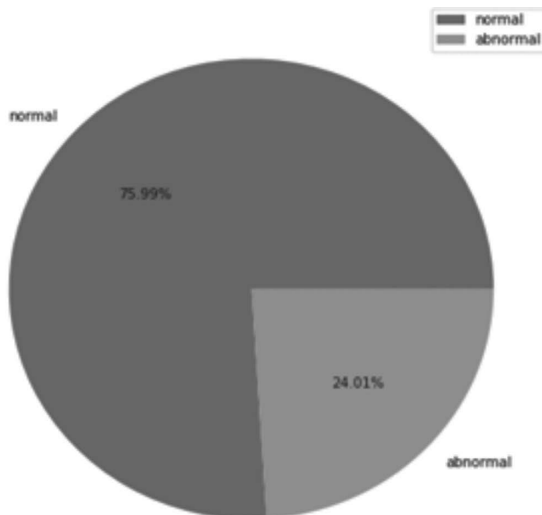


FIGURE 13.3 Normal and abnormal behavior.

TABLE 13.2
Accuracy Level of XGBoost, Naïve Bayes, Complement Naïve Bayes, AdaBoost, GaussianNB

Algorithms	Accuracy (%)
XGBoost	98.2507
Naïve Bayes	74.2655
Complement Naïve Bayes	92.2267
AdaBoost	98.3431
GaussianNB	74.2655

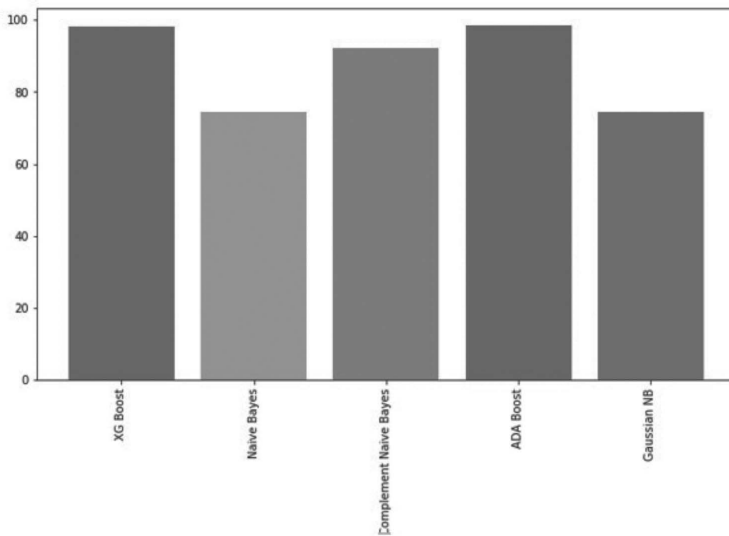


FIGURE 13.4 Comparative analysis of machine learning classifiers.

TABLE 13.3
Normal and Abnormal Behavior Using Metrics (Precision, Recall, F1-Score, and Support)

Metrics	Precision	Recall	F1-Score	Support
Abnormal	0.99	0.67	0.80	12326
Normal	0.48	0.98	0.65	3909

is better than with other techniques. Figure 13.4 gives a comparative analysis of machine learning classifiers.

Table 13.3 provides information about the metrics of normal and abnormal data traffic. Therefore, to check the performance of an intrusion detection system precision, recall, F1-score and support parameters are utilized.

13.6 COMPARATIVE DISCUSSION OF ML TECHNIQUES USING THE IDS

Table 13.4 presents a detailed comparative analysis using machine learning techniques for IoT-based IDS. Researchers have widely used machine learning techniques to identify cyber attacks, as well as the formation of a novel framework to design IDS for IoT networks.

TABLE 13.4
Comparative Analysis of Machine-Learning-Based IDS

Reference	Machine-Learning-Based IDS	Description
[40]	Anomaly-based	This work presents a framework based on three modules—capturing and logging, preprocessing, and a decision engine—thus showing higher accuracy and a lower false alarm rate.
[41]	Anomaly-based	Proposed geometric area analysis technique (GAA) for an anomaly-based detection system (ADS) based on the beta mixture model (BMM) with precise estimation is used for trapezoidal area estimation (TAE) for designing a light IDS.
[42]	Anomaly-based	Advance dataset is utilized, which includes nine categories of modern threat specimen. Overall, the work explains the issues related to datasets. In particular, statistical analysis, feature correlation examination, accuracy, and false alarm rates are used as metrics.
[43]	Hybrid	Old benchmark datasets are quite old for detecting some of the modern threats; so, facing these circumstances, the authors formulated a novel dataset regarding cyber attacks.
[44]	Anomaly-based	Authors simulated five NetFlow datasets to do experimentation.
[45]	Anomaly-based	Sensing botnet attacks can be analyzed using various protocols via a special framework consisting of a feature set, a feature selection and ensemble method is presented.
[46]	Anomaly-based	To combat known and zero-day attacks, a four-step strategy was proposed: gathering web attacks and network traffic, extracting important features, replicating web attack data, and detecting attacks.
[47]	Anomaly-based	The privacy of SCADA systems, having critical information, is a big challenge. This research work proposed a detection technique based on a correlation coefficient and expectation maximization clustering mechanism.
[48]	Anomaly-based	This paper has formulated a beta mixture technique, which is an anomaly method for attack detection.
[49]	Hybrid	The real-time surveillance and investigation of network-based attacks used a network forensic scheme. Therefore, the proposed system relies on capturing and storing network data, feature selection, and correntropy-variation technique.

TABLE 13.4 (Continued)
Comparative Analysis of Machine-Learning-Based IDS

Reference	Machine-Learning-Based IDS	Description
[50]	Signature-based	Botnets pose a serious threat within a network; to counter this problem, the ML technique for network forensics is used.
[51]	Hybrid	Authors proposed a new security system for Industry 4.0, which has two components; a smart management module and a threat intelligence module.
[52]	Anomaly-based	This research work has information to design and formulate a novel dataset. Development and application of many features rely on the evolution of decision engine (DE) techniques.

13.7 CONCLUSION AND FUTURE DIRECTIONS

Recently, artificial intelligence has been widely used to detect threats in many fields. The identification of an attack is considered a serious problem in IoT-based UAV networks. This chapter provides a comparative analysis to evaluate the intrusion detection system trust factor. Therefore, machine learning algorithms like XGBoost, naïve Bayes, complement naïve Bayes, AdaBoost, and GaussianNB are implemented using the UNSW-NB 15 dataset. Simulation is performed using Python. AdaBoost has better accuracy, about 98.3431%, in detecting cyber attacks. Also, XGBoost accuracy in identifying attack is 98.2507%. Overall, binary classification is used to check performance. In near future, optimization techniques will provide optimal solutions for detecting cyber attacks.

REFERENCES

- [1] Khan, Inam Ullah, Asrin Abdollahi, Ryan Alturki, Mohammad Dahman Alshehri, Mohammed Abdulaziz Ikram, Hasan J. Alyamani and Shahzad Khan. “Intelligent Detection System Enabled Attack Probability Using Markov Chain in Aerial Networks.” *Wireless Communications and Mobile Computing*, 2021 (2021).
- [2] Khan, I. U., I. M. Qureshi, M. A. Aziz, T. A. Cheema and S. B. H. Shah. “Smart IoT Control-Based Nature Inspired Energy Efficient Routing Protocol for Flying Ad Hoc Network (FANET).” *IEEE Access*, 8 (2020), pp. 56371–56378, <https://doi.org/10.1109/ACCESS.2020.2981531>.
- [3] Zhang, Shuowen, Yong Zeng and Rui Zhang. “Cellular-enabled UAV Communication: A Connectivity-constrained Trajectory Optimization Perspective.” *IEEE Transactions on Communications*, 67, no. 3 (2018), pp. 2580–2604.
- [4] Kim, J., S. Kim, C. Ju and H. I. Son. “Unmanned Aerial Vehicles in Agriculture: A Review of Perspective of Platform, Control, and Applications.” *IEEE Access*, 7 (2019), pp. 105100–105115, <https://doi.org/10.1109/ACCESS.2019.2932119>.
- [5] Abdollahi, Asrin and Mohammad Fathi. “An Intrusion Detection System on Ping of Death Attacks in IoT Networks.” *Wireless Personal Communications*, 112, no. 4 (2020), pp. 2057–2070.

- [6] R. Bassil, R. Hobeica, W. Itani, C. Ghali, A. Kayssi and A. Chehab, "Security Analysis and Solution for Thwarting Cache Poisoning Attacks in the Domain Name System," *2012 19th International Conference on Telecommunications (ICT)*, pp. 1–6, 2012, <https://doi.org/10.1109/ICTEL.2012.6221233>.
- [7] Yan, Q. and F. R. Yu. "Distributed Denial of Service Attacks in Software-defined Networking with Cloud Computing." *IEEE Communications Magazine*, 53, no. 4 (April 2015), pp. 52–59. <https://doi.org/10.1109/MCOM.2015.7081075>.
- [8] Zhang, K., X. Liang, R. Lu and X. Shen. "Sybil Attacks and Their Defenses in the Internet of Things." *IEEE Internet of Things Journal*, 1, no. 5 (October 2014), pp. 372–383. <https://doi.org/10.1109/JIOT.2014.2344013>.
- [9] Nassi, B., R. Bitton, R. Masuoka, A. Shabtai and Y. Elovici. "SoK: Security and Privacy in the Age of Commercial Drones." *2021 IEEE Symposium on Security and Privacy (SP)*, pp. 1434–1451, 2021, <https://doi.org/10.1109/SP40001.2021.00005>.
- [10] Garg, Sahil, Gagangeet Singh Aujla, Neeraj Kumar and Shalini Batra. "Tree-based Attack—Defense Model for Risk Assessment in Multi-UAV Networks." *IEEE Consumer Electronics Magazine*, 8, no. 6 (2019), pp. 35–41.
- [11] Ramadan, Rabie A., Abdel-Hamid Emara, Mohammed Al-Sarem and Mohamed Elhamahmy. "Internet of Drones Intrusion Detection Using Deep Learning." *Electronics*, 10, no. 21 (2021), p. 2633.
- [12] Zhang, C., P. Patras and H. Haddadi. "Deep Learning in Mobile and Wireless Networking: A Survey." *IEEE Communications Surveys & Tutorials*, 21, no. 3 (2019), pp. 2224–2287.
- [13] Aceto, G., D. Ciunzo, A. Montieri and A. Pescapé. "Mobile Encrypted Traffic Classification Using Deep Learning: Experimental Evaluation, Lessons Learned, and Challenges." *IEEE Transactions on Network and Service Management*, 16, no. 2 (2019), pp. 445–458.
- [14] Aceto, G., D. Ciunzo, A. Montieri and A. Pescapé. "Toward Effective Mobile Encrypted Traffic Classification Through Deep Learning." *Neurocomputing*, 409 (2020), pp. 306–315.
- [15] Shone, N., T. N. Ngoc, V. D. Phai and Q. Shi. "A Deep Learning Approach to Network Intrusion Detection." *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2, no. 1 (2018), pp. 41–50.
- [16] Marín, G., P. Casas and G. Capdehourat. "DeepSec Meets RawPower-deep Learning for Detection of Network Attacks Using Raw Representations." *ACM Sigmetrics Performance Evaluation Review*, 46, no. 3 (2019), pp. 147–150.
- [17] Wang, Yue, Yiming Jiang and Julong Lan. "FCNN: An Efficient Intrusion Detection Method Based on Raw Network Traffic." *Security and Communication Networks*, 2021 (2021).
- [18] Heady, R., G. Luger, A. Maccabe and M. Servilla. *The Architecture of Network Level Intrusion Detection System, Technical Report CS90–20, Department of Computer Science, University of New Mexico, 1990.*
- [19] Carter, E. *CCSP Self-Study: Cisco Secure Intrusion Detection System (CSIDS)*, Cisco Press, 2nd edition, 2004, ISBN-10: 9781587051449.
- [20] Anderson, D., T. Frivold and A. Valdes. Next-Generation Intrusion Detection Expert System (NIDES). A Summary, *SRI International Computer Science Laboratory Technical Report SRI-CSL-95–07, 1995.*
- [21] Silva, L. D. S., A. C. Santos, T. D. Mancilha, J. D. Silva and A. Montes. "Detecting Attack Signatures in the Real Network Traffic with ANNIDA." *Expert Systems with Applications*, 34, no. 4 (2008), pp. 2326–2333.

- [22] Patcha, A. and J. M. Park. "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends." *Computer Networks*, 51, no. 12 (2007), pp. 3448–3470.
- [23] Manikopoulos, C. and S. Papavassiliou. "Network Intrusion and Fault Detection. A Statistical Anomaly Approach." *IEEE Communications Magazine*, 40, no. 10 (2002), pp. 76–82.
- [24] Thomas, Rincy N. and Roopam Gupta. "Design and Development of an Efficient Network Intrusion Detection System Using Machine Learning Techniques." *Wireless Communications and Mobile Computing*, 2021 (2021).
- [25] Albulayhi, Khalid, Qasem Abu Al-Hajja, Suliman A. Alsuhibany, Ananth A. Jillepalli, Mohammad Ashrafuzzaman and Frederick T. Sheldon. "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method." *Applied Sciences*, 12, no. 10 (2022), p. 5015.
- [26] Thamilarasu, Geethapriya and Shiven Chawla. "Towards Deep-learning-driven Intrusion Detection for the Internet of Things." *Sensors*, 19, no. 9 (2019), p. 1977.
- [27] Dahou, Abdelghani, et al. "Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm." *Computational Intelligence and Neuroscience*, 2022 (2022).
- [28] Ren, Jiadong, et al. "Building an Effective Intrusion Detection System by Using Hybrid Data Optimization Based on Machine Learning Algorithms." *Security and Communication Networks*, 2019 (2019).
- [29] Einy, Sajad, Cemil Oz and Yahya Dorostkar Navaei. "The Anomaly-and Signature-based IDS for Network Security Using Hybrid Inference Systems." *Mathematical Problems in Engineering*, 2021 (2021), pp. 1–10.
- [30] Albulayhi, Khalid, et al. "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method." *Applied Sciences*, 12, no. 10 (2022), p. 5015.
- [31] Alzahrani, Abdulsalam O. and Mohammed J.F. Alenazi. "Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks." *Future Internet*, 13, no. 5 (2021), p. 111.
- [32] Verma, Parag, et al. "A Novel Intrusion Detection Approach Using Machine Learning Ensemble for IoT Environments." *Applied Sciences*, 11, no. 21 (2021), p. 10268.
- [33] Albulayhi, K., A. A. Smadi, F. T. Sheldon and R. K. Abercrombie. "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses." *Sensors*, 21 (2021), p. 6432.
- [34] Albulayhi, K. and F.T. Sheldon. "An Adaptive Deep-Ensemble Anomaly-Based Intrusion Detection System for the Internet of Things." In *Proceedings of the 2021 IEEE World AI IoT Congress (AllIoT)*, pp. 0187–0196, IEEE, Seattle, WA, 10–13 May 2021.
- [35] Eskandari, M., Z. H. Janjua, M. Vecchio and F. Antonelli. "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices." *IEEE Internet Things Journal*, 7 (2020), pp. 6882–6897.
- [36] Balogh, S., O. Gallo, R. Ploszek, P. Špaček and P. Zajac. "IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques." *Electronics*, 10 (2021), p. 2647.
- [37] Alrubayyi, H., G. Goteng, M. Jaber and J. Kelly. "Challenges of Malware Detection in the IoT and a Review of Artificial Immune System Approaches." *Journal of Sensor and Actuator Networks*, 10 (2021), p. 61.
- [38] Ambusaidi, M.A., X. He, P. Nanda and Z. Tan. "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm." *IEEE Transactions on Computers*, 65 (2016), pp. 2986–2998.

- [39] Albulayhi, Khalid, Qasem Abu Al-Haija, Suliman A. Alsuhibany, Ananth A. Jillepalli, Mohammad Ashrafuzzaman and Frederick T. Sheldon. "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method." *Applied Sciences*, 12, no. 10 (2022), p. 5015.
- [40] Moustafa, Nour, Gideon Creech and Jill Slay. "Big Data Analytics for Intrusion Detection System: Statistical Decision-Making Using Finite Dirichlet Mixture Models." In *Data Analytics and Decision Support for Cybersecurity*, pp. 127–156, Springer, Cham, 2017.
- [41] Moustafa, N., J. Slay and G. Creech. "Novel Geometric Area Analysis Technique for Anomaly Detection Using Trapezoidal Area Estimation on Large-Scale Networks." *IEEE Transactions on Big Data*, 5, no. 4 (1 December 2019), pp. 481–494. <https://doi.org/10.1109/TBDATA.2017.2715166>.
- [42] Moustafa, Nour and Jill Slay. "The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set." *Information Security Journal: A Global Perspective*, 25, no. 1–3 (2016), pp. 18–31.
- [43] N. Moustafa and J. Slay, "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set)," *2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015, <https://doi.org/10.1109/MilCIS.2015.7348942>.
- [44] Sarhan, M., S. Layeghy, N. Moustafa and M. Portmann. "Netflow Datasets for Machine Learning-Based Network Intrusion Detection Systems. arXiv 2020." *arXiv preprint arXiv:2011.09144*.
- [45] Moustafa, N., B. Turnbull and K. R. Choo. "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things." *IEEE Internet of Things Journal*, 6, no. 3 (June 2019), pp. 4815–4830, <https://doi.org/10.1109/JIOT.2018.2871719>.
- [46] Moustafa, N., G. Misra and J. Slay. "Generalized Outlier Gaussian Mixture Technique Based on Automated Association Features for Simulating and Detecting Web Application Attacks." *IEEE Transactions on Sustainable Computing*, 6, no. 2 (1 April–June 2021), pp. 245–256. <https://doi.org/10.1109/TSUSC.2018.2808430>.
- [47] M. Keshk, N. Moustafa, E. Sitnikova and G. Creech, "Privacy Preservation Intrusion Detection Technique for SCADA Systems," *2017 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2017, <https://doi.org/10.1109/MilCIS.2017.8190422>.
- [48] Moustafa, Nour, Gideon Creech and Jill Slay. "Anomaly Detection System Using Beta Mixture Models and Outlier Detection." In *Progress in Computing, Analytics and Networking*, pp. 125–135, Springer, Singapore, 2018.
- [49] Moustafa, Nour and Jill Slay. "A Network Forensic Scheme Using Correntropy-Variation for Attack Detection." In *IFIP International Conference on Digital Forensics*, pp. 225–239. Springer, Cham, 2018.
- [50] Koroniotis, N., N. Moustafa, E. Sitnikova and J. Slay. "December. Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques. In *International Conference on Mobile Networks and Management*, pp. 30–44, Springer, Cham, 2017.
- [51] Moustafa, N., E. Adi, B. Turnbull and J. Hu. "A New Threat Intelligence Scheme for Safeguarding Industry 4.0 Systems." *IEEE Access*, 6 (2018), pp. 32910–32924.
- [52] Moustafa, N., 2017. *Designing an Online and Reliable Statistical Anomaly Detection Framework for Dealing with Large High-Speed Network Traffic* (Doctoral dissertation, UNSW Sydney).

14 Blockchain Solutions for Cyber Criminals

*Vijendra Kumar Maurya, Denis Jangeed,
Latif Khan, and Bhupendra Kumar Soni*

14.1 INTRODUCTION

The next generation will be born into a world that is more connected than ever. They will grow up with smartphones, social media, and the Internet of Things and will be exposed to a vast amount of information and data. While these advancements bring many benefits, they also pose significant security risks that need to be addressed. One of them, a distributed network called a blockchain, has millions of users worldwide. The blockchain is accessible to all users, and all of the data there is encrypted for security. It is the responsibility of all other participants to confirm the accuracy of the data posted to the blockchain. It's a digital, distributed, and decentralized public ledger that makes it possible to track assets and record transactions in a corporate network. Blockchain technology is a digital ledger system that allows several parties to access, verify, and update information in a secure and transparent way [1]. It was first announced in 2008 by an anonymous person or group under the pseudonym Satoshi Nakamoto, as the underlying technology behind the crypto currency, Bitcoin. However, since then, blockchain technology has expanded to a wide array of industries, including healthcare, finance, and logistics, due to its numerous benefits. One of the important advantages of blockchain technology is its immutability. Due to numerous intrusions in almost every industry, cyber security has recently grown to be a significant problem [12]. Once information is added to the blockchain, it cannot be altered or deleted without the consensus of the network. This makes it an ideal technology for storing and sharing sensitive data, such as medical records or financial transactions, without the need for intermediaries like banks or governments. Another benefit of blockchain technology is its decentralized nature. Rather than having a central authority control the network, blockchain is distributed across multiple nodes, making it difficult for any one party to manipulate the data. This enhances security and makes it a more democratic technology. Additionally, blockchain technology is transparent, allowing anyone with access to the network to view all transactions on the ledger. This can increase trust and accountability among parties and prevent fraud and corruption. The potential applications of blockchain technology are vast and varied. In healthcare, for example, blockchain can be used to securely store and share patient medical records among healthcare providers, improving patient care and reducing costs. In finance, blockchain can be used to facilitate cross-border payments and reduce transaction times and costs. As blockchain technology continues to

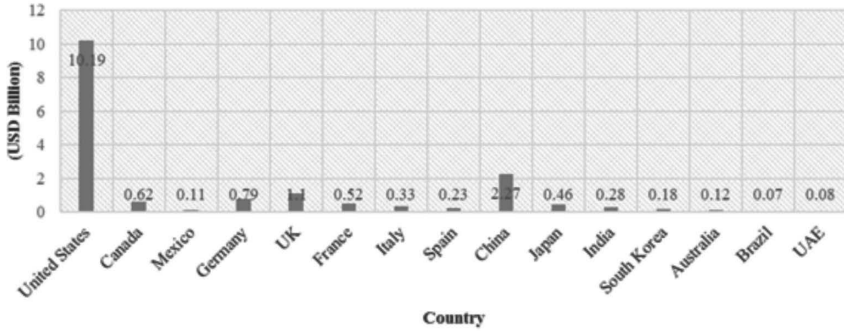


FIGURE 14.1 Blockchain technology market size (US\$billion).

evolve and gain wider adoption, it has the potential to revolutionize the way we store and share information across industries [2]. Also, we can say that blockchain technology has been a game changer in the world of cyber security, offering unprecedented levels of security and transparency. It is a decentralized, distributed digital ledger that allows multiple parties to verify, access, and update information in a secure and transparent manner. With the rise of cyber crime, blockchain technology has become an essential tool for cyber security professionals to secure data, detect and prevent fraudulent activity, and mitigate other security risks. This chapter will explore the applications of blockchain technology in cyber security, along with the security solutions it offers [3]. The information on the global blockchain technology market size in different countries, as reported by Verified Market Research in 2021.

Figure 14.1 shows information on the estimated market size for the year 2020 and is subject to change as the market evolves.

14.2 ROLE OF BLOCKCHAIN TECHNOLOGY FOR BOOSTING OF ECONOMY

Blockchain technology has the potential to significantly boost the economy by improving efficiency, reducing costs, and increasing transparency. The technology’s decentralized, secure, and transparent nature makes it ideal for a variety of uses in the business world, including finance, supply chain management, and identity verification. The potential to revolutionize the finance industry is that of reducing transaction costs, improving efficiency, and increasing transparency. For example, blockchain-based systems can enable faster, cheaper, and more secure cross-border payments, which can reduce costs for businesses and consumers alike. Additionally, blockchain can enable the creation of decentralized financial instruments like smart contracts and decentralized autonomous organizations (DAOs), which can potentially lower the need for intermediaries and enhance effectiveness. Blockchain can also be used to improve supply chain management by creating a secure and transparent ledger that tracks the movement of goods from origin to destination. This can help reduce fraud, counterfeiting, and theft, as well as improve the efficiency of the

supply chain by reducing paperwork and manual processes. Creating a decentralized, secure, and tamper-proof system that stores and verifies identity information can help reduce identity theft, fraud, and data breaches and can increase efficiency by eliminating the need for intermediaries like banks and governments to manage identity data. Decentralized centralized applications built on blockchain technology can also boost the economy by creating new business models and revenue streams [9]. For example, decentralized applications (dApps) can enable peer-to-peer marketplaces that connect buyers and sellers directly, reducing the need for intermediaries and increasing efficiency. Additionally, dApps can enable new types of business models, such as decentralized autonomous organizations (DAOs), which can operate without centralized leadership or ownership. Finally, blockchain technology can enable the creation of digital tokens that represent assets like real estate, art, and stocks. This can unlock trillions of dollars in value by making these assets more accessible and tradable. Additionally, tokenization can enable new types of crowd funding models that allow businesses raise capital from a global pool of investors.

14.3 BLOCKCHAIN TECHNOLOGY MARKET

In the past few years, the market for blockchain technology has been experiencing rapid growth due to a rising need for secure and transparent digital transactions across various industries. According to a report by Markets and Markets, the global blockchain technology market is projected to grow from US\$1.57 billion in 2019 to US\$9.2 billion by 2025, at a CAGR of 44.5% during the forecast period shown in Table 14.1. One of the key factors driving this growth is the increasing adoption of blockchain technology by businesses and governments around the world. According to a report by Deloitte, over 50% of surveyed companies in the United States are now using or considering blockchain technology, up from just 13% in 2016.

The financial services industry has been one of the earliest and most active adopters of blockchain technology, with applications ranging from cross-border payments to securities trading and settlement. However, blockchain technology is also being

TABLE 14.1
Global Blockchain Technology Market Size (2019–2025)

Year	Global Blockchain Technology Market Size
2019	US\$1.57 billion
2020	US\$3.0 billion
2021	US\$3.67 billion
2022	US\$4.9 billion
2023	US\$6.3 billion
2024	US\$7.7 billion
2025	US\$9.2 billion

Source: Markets and Markets.

used in a wide range of other industries, including healthcare, supply chain management, and digital identity verification. In terms of geographic distribution, the blockchain technology market is expected to be dominated by North America, followed by Europe and Asia Pacific [7].

According to a report by Grand View Research, North America accounted for 40% of the global blockchain technology market in 2020, as shown in Figure 14.2, with Europe and Asia Pacific following at 32 and 24%, respectively, as shown in Figure 14.3.

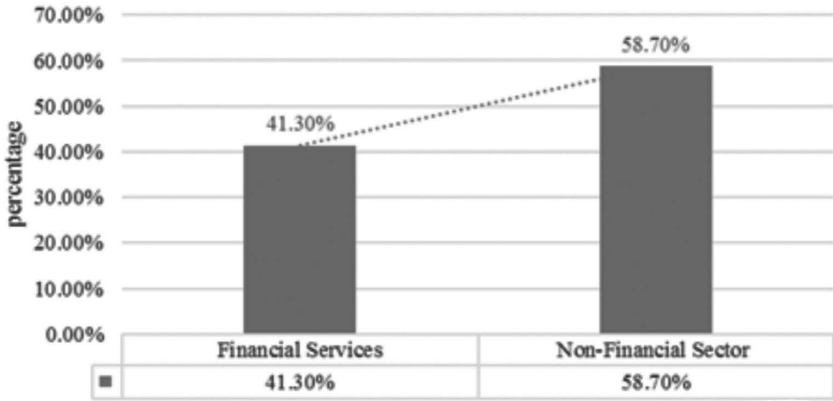


FIGURE 14.2 Global blockchain technology market by application (2020). (Source: Statistics generated from Statista and represented as a graph by authors.)

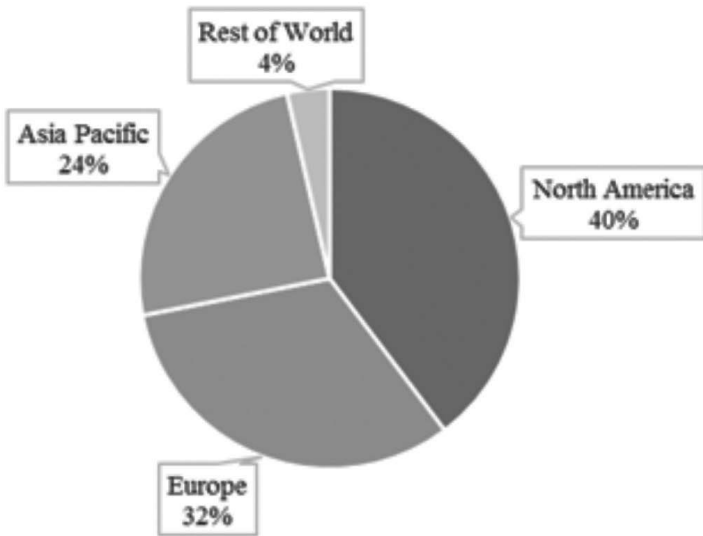


FIGURE 14.3 Global blockchain technology market by region (2020). (Source: Statistics generated from Grand View Research and represented as a graph by authors.)

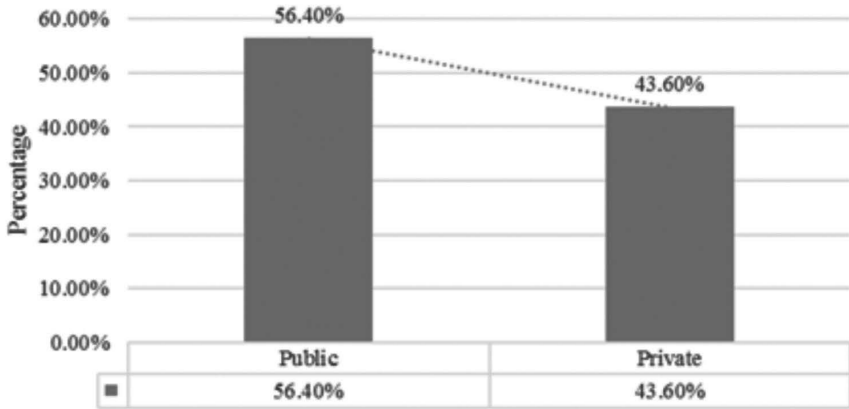


FIGURE 14.4 Global blockchain technology market by region (2020). (Source: Statistics generated from Allied Market Research and represented as a graph by authors.)

In addition to traditional public blockchain platforms like Bitcoin and Ethereum, there has been a growing trend toward private and permission blockchain networks, which offer greater privacy and control over data [4]. According to a report by Allied Market Research, the private blockchain segment is expected to grow at a higher CAGR of 43.6% during the forecast period compared to the public blockchain segment, as shown in Figure 14.4. In general, the blockchain technology market is expected to continue to grow rapidly in the coming years, driven by increasing demand for secure, transparent, and efficient digital transactions across a wide range of industries [8].

14.4 APPLICATIONS OF BLOCKCHAIN TECHNOLOGY IN CYBER SECURITY

Blockchain technology can be applied in several areas of cyber security to improve security, as discussed next.

14.4.1 SECURE DATA STORAGE

Blockchain can be used to securely store sensitive data, such as medical records, financial data, and private information. The immutability and decentralization of the blockchain make it difficult for hackers to gain unauthorized access or to tamper with data stored on the chain.

14.4.2 FRAUD DETECTION AND PREVENTION

Blockchain can be used to detect and prevent fraudulent activity, such as identity theft and financial fraud. The transparency of the blockchain allows all parties to view transactions, making it easier to detect fraudulent activity.

14.4.3 SUPPLY CHAIN SECURITY

Blockchain can be used to secure the supply chain by creating a transparent and immutable record of all transactions. This makes it easier to detect and prevent fraud, theft, and counterfeiting [11].

14.4.4 DECENTRALIZED IDENTITY MANAGEMENT

Blockchain can be used to create a decentralized identity management system that eliminates the need for intermediaries like banks and governments to manage identity data. This reduces the risk of identity theft and data breaches.

14.5 SECURITY ISSUE INVOLVED IN BLOCKCHAIN TECHNOLOGY

While blockchain technology is considered highly secure, some security issues still need to be addressed. Here are some of the most significant security issues involved in blockchain technology: 51% attack, smart contract vulnerabilities, private key theft, malware and phishing attacks, forking, ICO fraud. etc. In a 51% attack, a single entity or group of entities control 51% or more of the computing power on a blockchain network. This allows them to manipulate transactions, double-spend coins, and reverse previously confirmed transactions. In smart contract vulnerabilities, smart contracts are self-executing programs that run on a blockchain. These contracts can contain vulnerabilities, such as coding errors, which can be exploited by attackers to steal funds or disrupt the network. A private key is a secret code that is used to access and transfer crypto currencies stored in a blockchain wallet. If a private key is stolen, the attacker can access and transfer the funds without the owner's permission. Attackers can use malware or phishing attacks to gain access to a user's computer or mobile device and steal their private keys or other sensitive information. Forking occurs when a blockchain network splits into two separate networks due to a disagreement over the rules or governance of the network. This can result in a loss of trust and value for the network's users. Initial coin offerings (ICOs) are a popular way for startups to raise funds through the sale of new crypto currencies. However, many ICOs are fraudulent, and investors can lose their money if they invest in a fake or scam ICO. To mitigate these security issues, blockchain developers and users should implement strong security measures such as multifactor authentication, encryption, and regular security audits. Additionally, education and awareness among users can also help to prevent security breaches and fraud on the blockchain network [5, 6].

14.6 SECURITY TYPES REQUIRED IN BLOCKCHAIN SYSTEM

The main focus of blockchains lies in the three fundamental security concepts of confidentiality, integrity, and availability. In essence, blockchain is a distributed system that ensures availability and maintains data integrity by allowing all nodes to agree based on a chain of transactions. It is possible to protect the confidentiality of transactions with the use of suitable cryptographic keys. A holistic approach in

blockchain systems covers security from unauthorized insiders, hacked nodes, or server failure. It also includes the authentication and authorization of entities using the blockchain, transaction transparency, verification, and communication infrastructure security [9]. Blockchain systems should primarily consider the following areas of security:

1. Network-level security
2. Transaction-level security
3. Ledger-level security.
4. Associated surround system security
5. Smart contract security

From a network perspective, communication between parts of various nodes must be secure. It must be protected against a variety of network-wide internal and external attack vectors. The ledger ought to be able to survive denial of service attacks. Public surround sound systems are not inherently vulnerable to security risks, but some security issues are associated with them that users should be aware of. Surround sound systems can be connected to a home network, which can be vulnerable to attacks if not properly secured. This can allow attackers to gain access to the network and potentially control the surround sound system. If the surround sound system is not properly secured, unauthorized users may be able to access it and control it remotely. This can include changing the volume, altering the sound quality, or even turning the system off. In some cases, attackers may be able to eavesdrop on conversations or other audio content that is transmitted through the surround sound system. This can be a particular concern if the system is used for business or other sensitive purposes. Smart contracts are a key feature of blockchain technology that enable the execution of complex agreements and transactions in a secure and decentralized way. While smart contracts are designed to be highly secure, some security risks are still associated with them. Here are some of the key security considerations for smart contracts in blockchain:

1. **Code Vulnerabilities:** Smart contracts are written in programming languages like Solidity, which can contain coding errors or vulnerabilities that can be exploited by attackers. These vulnerabilities can allow attackers to steal funds, manipulate transactions, or disrupt the network.
2. **Contract Execution Risks:** Smart contracts can execute automatically based on predefined conditions. If these conditions are not properly set up, it can lead to unintended consequences or unexpected behavior, which can result in financial losses.
3. **Oracle Risks:** Smart contracts rely on external data sources called oracles to access real-world data. If oracles are not properly secured, they can be manipulated to provide false or misleading data, which can result in incorrect contract execution and financial losses.
4. **Governance Risks:** Smart contracts are often deployed on decentralized networks where there is no central authority or governance. This can lead to governance risks, such as disputes over contract terms, disagreements over contract execution, or malicious actions by network participants [10].

14.7 SECURITY SOLUTIONS OFFERED BY BLOCKCHAIN TECHNOLOGY

Security is an important issue. Given the cyber threats, numerous blockchain-technology-based solutions are available.

14.7.1 ENCRYPTION

Blockchain uses public key cryptography to encrypt data stored on the chain, making it difficult for hackers to access and decipher the data.

14.7.2 CONSENSUS MECHANISMS

Consensus mechanisms are used in blockchain to ensure that all nodes on the network agree on the state of the blockchain. This prevents attacks such as double-spending or the 51% attack.

14.7.3 MULTIFACTOR AUTHENTICATION

When accessing the blockchain, multifactor authentication (MFA) is a security protocol that necessitates users to provide more than one form of authentication, such as a password and biometric authentication like facial recognition or fingerprint scanning.

14.7.4 PERMISSIONED BLOCKCHAIN

Permission blockchain restricts access to the network to only trusted parties, which increases security. This is useful for sensitive industries, such as healthcare or finance.

14.7.5 REGULAR AUDITING

Regular auditing is necessary to ensure that the blockchain network is secure. This includes monitoring the network for anomalies and irregularities and reviewing access controls to ensure that only authorized parties have access to the blockchain.

On addition, other security solutions should also be considered. Public key interface (PKI) ideas must be used to encrypt transactions to prevent data compromise with unauthorized parties. Identification and transaction creation authorization must be protected; therefore only a specific name should be used. Only authorized members are permitted to use the blockchain. The blockchain's multi-signature capability is available for sensitive transactions, and the transaction information cannot be changed or altered. Valid participants start transactions in the network, and the members' transaction must be signed. "X" must be able to do transactions only under that name. To mitigate associated surrounding security issues, users should take steps to properly secure their network and ensure that their surround sound system is protected with a strong password. It is also important to keep the system's firmware and

software up-to-date to ensure that any known vulnerabilities are addressed. Finally, users should be cautious when connecting their system to public Wi-Fi networks, as these are often unsecured and can be vulnerable to attacks. To mitigate smart contract security risks, developers and users of smart contracts should follow best practices for secure contract development, such as code audits, testing, and formal verification. Additionally, they should use trusted oracles and follow best practices for contract execution and governance, such as using multi-signature wallets and establishing dispute resolution mechanisms. Finally, they should stay up-to-date on the latest security vulnerabilities and best practices in smart contract development and deployment.

14.8 CONCLUSION

Blockchain technology has the potential to significantly boost the economy by improving efficiency, reducing costs, and increasing transparency. Its applications in finance, supply chain management, identity verification, and decentralized applications, as well as its ability to enable tokenization of assets, make it an essential tool for businesses looking to stay competitive in today's rapidly evolving digital landscape. As blockchain technology continues to mature and gain wider adoption, it will play an increasingly important role in driving economic growth and innovation. Its applications in cyber security, such as secure data storage, fraud detection and prevention, supply chain security, and decentralized identity management, make it an essential tool for cyber security professionals. The security solutions offered by blockchain technology, such as encryption, consensus mechanisms, multifactor authentication, permission blockchain, and regular auditing, enhance the security of the blockchain network and protect against security threats. As blockchain technology continues to evolve and gain wider adoption, it will continue to play an increasingly important role in cyber security.

REFERENCES

- [1]. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Retrieved from <https://bitcoin.org/bitcoin.pdf>
- [2]. Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media.
- [3]. Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin.
- [4]. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. *Applied Innovation*, 2(6–10), 71–81.
- [5]. Markets and Markets. (2020). Blockchain Technology Market by Component, Application (Digital Identity, Payments, Smart Contracts, Supply Chain Management, and Others), Organization Size, Deployment Mode, Vertical (BFSI, Government, Healthcare and Life Sciences, Real Estate), and Region—Global Forecast to 2025. Technical Report [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/>
- [6]. Deloitte. (2019). 2019 Global Blockchain Survey. Technical Report [Online]. Available: <https://www2.deloitte.com/fr/fr/pages/services-financier/articles/global-blockchain-survey-2019.html>

- [7]. Grand View Research. (2021). Blockchain Technology Market Size, Share & Trends Analysis Report by Type (Public, Private), By Application (Financial Services, Healthcare, Media & Entertainment), By Region, and Segment Forecasts, 2020–2027. Technical Report [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/>
- [8]. Allied Market Research. (2020). Blockchain Technology Market by Type (Public, Private, and Hybrid), Component (Infrastructure and Protocol), Application (Digital Identity, Payments, Smart Contract, Supply Chain Management, and Others), and Industry Vertical (BFSI, Government, Healthcare and Life Sciences, Energy and Utilities, Telecom, Media and Entertainment, Retail and E-Commerce, Automotive, and Others): Global Opportunity Analysis and Industry Forecast, 2020–2027. Technical Report [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/>
- [9]. Aruna, P. S. G., & Lalitha Bhaskari, D. (2018). A Study on Blockchain Technology. *International Journal of Engineering & Technology*, 7(2.7), 418–421.
- [10]. Watanabe, H., Fujimura, S., Nakadaira, A., Miyazaki, Y., Akutsu, A., & Kishigami, J. (2016, Jan.). “Blockchain Contract: Securing a Blockchain Applied to Smart Contracts,” in *IEEE International Conference on Consumer Electronics (ICCE’16)*, IEEE, Las Vegas, NV, USA, pp. 467–468.
- [11]. Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). “On the security and performance of proof of work blockchains,” in *Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS’16)*, New York, NY, ACM, 2016, pp. 3–16.
- [12]. Saxena, R., & Gayathri, E. (2022, Jan. 1). Cyber Threat Intelligence Challenges: Leveraging Blockchain Intelligence with Possible Solution. *Materials Today: Proceedings*, 51, 682–689.

15 Blockchain Security Measures to Combat Cyber Crime

Rahmeh Ibrahim and Qasem Abu Al-Haija

15.1 INTRODUCTION

Both the business world and academia have recently paid close attention to cryptocurrencies. By 2023, the capital market for Bitcoin, frequently referred to as the first cryptocurrency, will reach US\$24 million [1]. Bitcoin's main working component is the blockchain. The year 2009 saw the implementation of a proposal that had first surfaced in 2008. All committed transactions are kept in a chain of blocks in a public ledger called the blockchain. This chain expands each time a new block is added. The decentralization, persistence, anonymity, and audibility of blockchain technology are significant characteristics [2].

Blockchain can work in a decentralized setting because it combines several important technologies, such as distributed consensus mechanisms, digital signatures based on asymmetric cryptography, and cryptographic hashing. A transaction can be carried out decentralized using blockchain technology. Blockchain has the potential to cut costs while also greatly boosting efficiency. Blockchain technology can be used for various things besides cryptocurrencies, even though Bitcoin is the most well-known application. Digital assets, remittances, and online payments are just a few financial services that can benefit from using blockchain because it eliminates the need for a bank or other intermediary [3, 4].

The next generation of Internet interactions comprises IoT, smart contracts, public utilities, reputation mechanisms, and security provisions. One of the most promising methods for doing this is blockchain technology [5–7].

Even though blockchain technology has great potential for creating new Internet infrastructure, it is plagued by several technical problems. First, scalability is a significant issue. A new block of Bitcoin is mined every 10 minutes, and block sizes are currently restricted to 1 MB. As a result, Bitcoin can only process 7 transactions/second, making it unfit for high-frequency trading. Second, a selfish mining strategy has been shown to allow miners to profit beyond their fair share of earnings [8]. To increase their future earnings, miners hide their extracted blocks. As a result, branches may frequently happen, halting the growth of the blockchain.

One new way to fight the pervasive threat of cyber crime that blockchain makes possible is the ability to protect data storage. Institutions and businesses can stop

data theft using distributed ledgers or record technology to store and share information. Distributed records make it possible to hash, encrypt, and decentralize information [6]. Consider it like a 1,000-piece puzzle. A hacker can access all 1,000 pieces simultaneously by breaking into a centralized system. In practice, one security lapse allows someone to obtain the private information of about a thousand people.

Cyber criminals can access only a single component of a decentralized system at a time, making it difficult and time-consuming to get the full picture. To get a person's personal information, they must hack into many different gateways repeatedly, which enables sufficient time to verify the weakness and stop the attack [6]. To protect essential outward communications, such as domain name services (DNS), this concept can also be used to create distributed network security.

The 2016 attack that brought down Twitter and Spotify exposed the vulnerability of the current DNS protocol, which depends on caching and maintains the access key on just one server [9]. A blockchain-based server would reduce the risk by establishing a wider network of security keys. Imagine a chest with several locks. Before any of the locks can be opened, they must first be unlocked using a variety of keys that could be hidden anywhere. This logic is the foundation for the decentralized approach to network security [10]. From the cyber security perspective, blockchain technology offers us a fresh perspective on designing systems that thwart cyber attacks. It is similar to the distinction between a community that keeps all its funds in a single bank and individuals who keep their funds at home. Despite having security measures in place, banks continue to be a top target for robbers looking to flee with a sizable sum of cash.

15.2 BLOCKCHAIN TECHNOLOGY BACKGROUND

The data structure offered by blockchain technology possesses inherent security features like decentralization, cryptography, and consensus, ensuring the authenticity of transactions. Its potential applications are vast and diverse, encompassing areas such as health, finance, smart production, IoT, and others.

15.2.1 BLOCKCHAIN TECHNOLOGY

Satoshi Nakamoto initially introduced blockchain [11] to tackle the issues associated with the traditional payment system, which relies on a third party to authenticate and verify transactions between parties. In contrast, blockchain is a public and decentralized database where records are shared and replicated across multiple nodes in a peer-to-peer (P2P) network. Transactions are recorded in unalterable blocks that form an immutable chain of records.

The current digital economy relies on a trusted third party to conduct secure transactions, but because these parties are vulnerable to hacking or manipulation, blockchain technology has emerged [12]. Motivated by the idea of Bitcoin, blockchain can be implemented in finance, national governance, business operations, education, medicine, and other non-financial areas because of its benefits, such as decentralization, persistence, trust, immutability, anonymity, and audibility.

The term “blockchain” refers to a technology that provides security and a distributed database that can replace the traditional database to provide services without a centralized authority or administrator. It uses a cryptographic algorithm to validate the transactions and allows assets to be transferred directly without third parties.

One of blockchain’s most important applications is Bitcoin, a digital transfer technology. This transaction is broadcast to all, and then the transaction is validated using a cryptography algorithm called Proof of Work (POW), which is a very complex puzzle that is added to the chain as a new block. The node that solves this puzzle is called miner, and it’s getting the right to add a block to the chain and be rewarded. To be a miner in the Bitcoin network, it’s not necessary to have a certification; anyone can become a miner, but they need to download the software that needs to be mined and must have powerful computing power devices to solve the puzzle.

15.2.2 BLOCKCHAIN TECHNOLOGY ARCHITECTURE

15.2.2.1 Block Components

A blockchain is composed of individual blocks, with each block comprising a header and a body, as shown in Figure 15.1. The block header contains a set of components:

- **Merkle Tree Root:** This is a binary tree used to increase the efficiency of the validation data process.
- **Timestamp:** This value is indicated when this block is created.

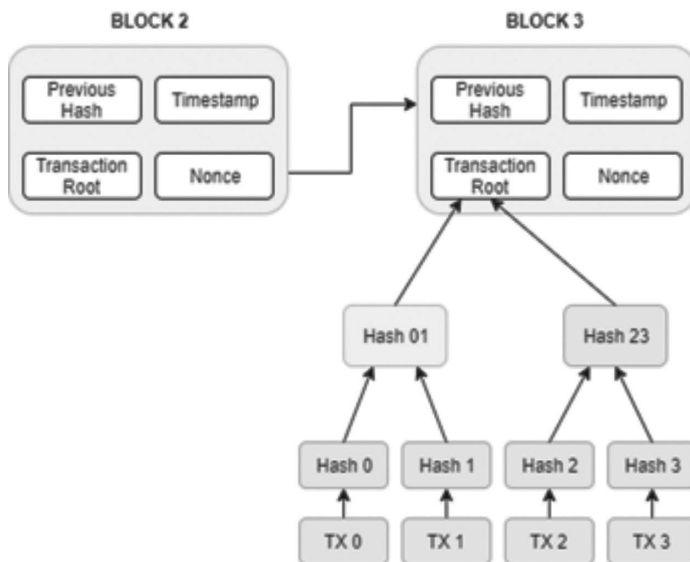


FIGURE 15.1 Block structure in blockchain technology.

- **Previous Hash Block:** The hash value of each block is generated by a hash function and used to link the block with its preceding block in the chain, safeguarding the chain against any changes.
- **Nonce number:** An integer number between 32 and 64 bits.

The block body holds all the transactions, and the number of transactions that can fit in a block depends on the size of the block and each transaction. Public key (asymmetric) cryptography is utilized by blockchain to authenticate transactions [19]. Digital signatures are retained in unreliable circumstances. In the following section, we will briefly overview digital signatures.

15.2.2.2 Blockchain Technology and Digital Signatures

Both a private key and a public key are available to each user. The private key is used to sign transactions. All network participants can access the public keys used to obtain the distributed digitally signed transactions across the network. A blockchain digital signature is shown in Figure 15.2. The majority of digital signatures have two steps: signing and verifying.

Let us use Figure 15.1 as an example again. Prior to signing a transaction, Alice generates a hash value by utilizing the transaction’s information. She then encrypts this hash value with her private key and transmits it to a different user. To confirm the received transaction, Bob combines the original data with the hash and decrypts it. He authenticates the transaction by comparing the decrypted hash, obtained using Alice’s public key, with the hash value calculated by Alice from the data, using the same hash function. Currently, one of the most prevalent digital signature algorithms in use is ECDSA [20].

15.2.3 HOW BLOCKCHAIN TECHNOLOGY WORKS

Cryptocurrency applications like Bitcoin are the first to use a blockchain as a platform. When someone needs to transfer money from your account to another using Bitcoin, the request transaction steps are shown in Figure 15.3:

- A digitally signed transaction is broadcast to every node or computer in the peer-to-peer (P2P) network.

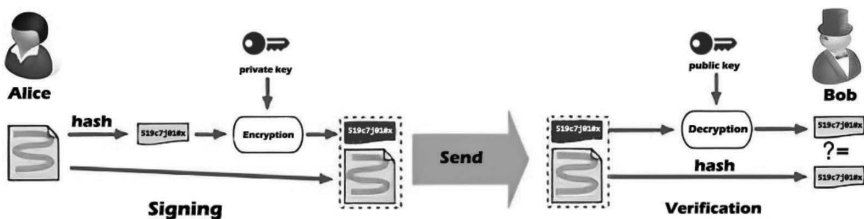


FIGURE 15.2 Blockchain and digital signature. (see Ref. [21]).

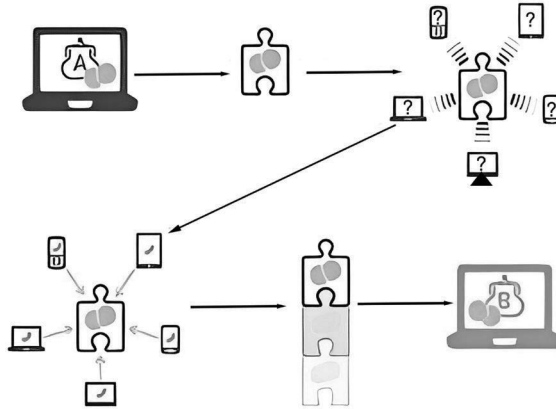


FIGURE 15.3 How blockchain technology works. (see Ref. [16]).

- Using a consensus algorithm called Proof of Work, the nodes validate the transaction after receiving it (POW).
- A new block is added if the transaction is valid.
- The deal is successfully finished.

In blockchain, before the transaction is broadcast to all nodes, each node must solve a difficult mathematical problem or puzzle called POW; the first node to solve this puzzle is called the “miner node,” and this node gets a Bitcoin as a reward.

15.2.4 BLOCKCHAIN TECHNOLOGY FEATURES

Blockchain technology creates many advantages in all fields and areas used because of its features. Blockchain has multiple features:

- **Decentralized:** This means all data processes like storage, maintenance, verification, and sharing are based on a distributed system structure, and the trust between these nodes is built by mathematical methods or puzzles rather than third-trusted parties [17].
- **Immutability:** All data stored in this chain after being entered in a block can't be erased or modified. This property has two reasons [13]. First, each block in the chain is linked to the previous block by the hash value, so if any transaction is modified or deleted, then this hash value is changed, and this affects all the previous blocks. This process takes great power and high cost. Second, this chain is replicated in all nodes in the P2P network. It must be synchronized among all nodes, so that every node in the chain is modified. Hence, all chains in the network need to be modified, and this is impossible because the attacker needs to control and change over 51% of the chains stored in the network. This process is known as the Sybil attack [14].
- **Traceability:** All transactions are stored in the blockchain in chronological order, so the trace process of any transaction is simple and easy.

- **Anonymity:** Each node in the blockchain has a fake name so that no one can trace any nodes and their data.
- **Transparent:** All data stored in the blockchain is transparent for each node in the network because any node can update the chain and add a new block successfully [18].

15.2.5 BLOCKCHAIN TECHNOLOGY TYPES

Depending on the users they have in various fields, blockchain can be divided into three types:

- **Public Blockchain:** This pertains to the permissionless blockchain, where all nodes within a peer-to-peer network have access to the content stored on the chain and employ a consensus algorithm such as Proof of Work (POW) or Proof of Stake (POS) to authenticate transactions. Also, storing sensitive information like medical or military records in this chain type is impossible because the chain's confidentiality cannot be guaranteed; see Figure 15.4(A). A public blockchain is an example, such as the Ethereum platform [15].
- **Consortium Blockchain:** Also known as a permission blockchain, this type necessitates the validation of a transaction by two or more entities before it can be appended to the chain, as illustrated in Figure 15.4(B). The authority to verify data on the chain is limited to a group of nodes in this type. The storage of electronic medical records uses this type in many sensitive industries, including healthcare (EMRs).
- **Private Blockchain:** This pertains to permissioned blockchain, where the authorization to write and validate data on the chain is limited to a single organization. However, the permission to access this data can be either public or private, contingent on the type of organization. Moreover, the Proof of Work (POW) or Proof of Stake (POS) consensus algorithms are not mandatory in this type of agreement. Rather, the Proof of Authority (POA) consensus algorithm is utilized (see Figure 15.4(C)).

15.2.6 BLOCKCHAIN TECHNOLOGY LIMITATIONS

15.2.6.1 Scalability

As more transactions are made, the blockchain becomes heavier. More than 100 GB of storage is currently available on the Bitcoin blockchain. Each transaction needs to be saved so that it can be validated. The preliminary constraint on block size and the interval to produce a new block also inhibit Bitcoin from the real-time handling of millions of transactions. It can only handle about seven transactions per second. Many small transactions may experience delays due to the extremely low block capacity, as miners favor those with an excessive transaction charge.

15.2.6.2 Privacy Leakage

Because transactions on blockchain are never made using users' real identities, this technology is extremely secure. If information leaks, users might also generate a

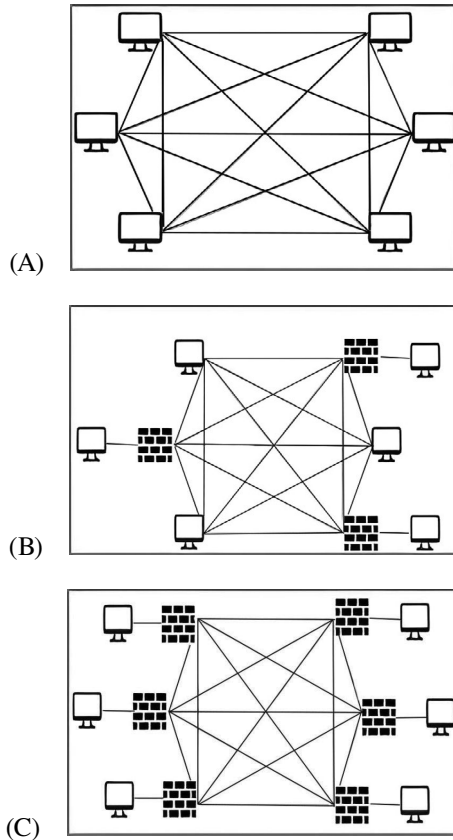


FIGURE 15.4 (A) Public blockchain technology, (B) consortium blockchain technology, and (C) private blockchain technology.

large number of addresses; blockchain cannot guarantee transactional privacy [22]. Additionally, personal information may be linked to a user’s Bitcoin transactions. Additionally, [23] has provided a technique for establishing a connection between IP addresses and user pseudonyms; even with the protection of firewalls or network address translation (NAT), users may still be vulnerable.

15.2.6.3 Selfish Mining

Malicious, self-serving miners may launch attacks on the blockchain. According to the consensus, nodes with more than 51% of the total computing power can jeopardize the transaction and the blockchain. Recent studies, however, indicate that even nodes with less than 51% power might still be dangerous [24]. In particular, the network is still at risk even if only a small amount of hashing power is used to cheat. Selfish miners would keep their mined blocks without broadcasting since the private branch could only be made public under specific conditions.

All miners will accept the private branch because it is longer than the current public chain. Before the private blockchain is published, unethical miners expend time

and resources on a pointless branch, while egotistical miners mine private chains without rivals. Consequently, egotistical miners frequently profit more. The egotistical pool would quickly gain 51% power as logical miners would join it. As evidence of how unreliable blockchain technology is, many additional attacks are built on selfish mining. By non-trivially fusing network-level eclipse attacks with mining attacks in stubborn mining, miners can boost their profit [25].

Miners will still use the trail tenacity strategy to mine the blocks even if the private chain is abandoned. Sometimes, though, it can result in 13% gains over competitors without a stubborn trail. Compared to pure selfish mining, there are selfish mining techniques that, according to [25], are more lucrative and profitable for smaller miners. However, the gains are insignificant. It also shows how selfish mining can still be lucrative for attackers with less than 25% of the computational resources.

To address the issue of selfish mining, Heilman [26] provided a cutting-edge method for honorable miners to choose which branch to follow. If beacons and timestamps were random, honest miners would pick more new blocks. However, [26] is vulnerable to fake timestamps. The network must generate and approve every block within a set amount of time, according to the fundamental tenet of [27]. Selfish miners are limited to getting the payment that ZeroBlock anticipates.

15.3 CYBER CRIMES

15.3.1 OVERVIEW

Cyberspace involves digital network communication. Sensitive information can be transmitted over networks, attracting adversaries looking to steal information. Therefore, the information transmitted and the network must be secure. Because cyberspace is not immune to attacks, cyber security is required. Cyber crime is the umbrella term for all criminal events implying a digital system such as a computer, network, or digital tools. Cyber crimes are defined as behaviors such as hacking, spamming, phishing, identity theft, unauthorized access, etc., whereas computers, laptops, mobile devices, or any other digital devices that facilitate cyber crimes are defined as objects of crime. A person, group, or organization that engages in cyber crime is called a cyber criminal, and they frequently use computers as tools, targets, or both. Some forms of cyber crime are:

- Email and Internet scams.
- Identity theft (where personal information is stolen and exploited).
- Theft of financial or credit card information.
- Theft and illicit sale of business-related data.
- Cyber extortion (the act of demanding money to prevent a threatened online attack).
- Attacks using ransomware (cyber extortion), a type of cyber extortion.
- Cryptojacking (the practice of hackers mining cryptocurrency using resources not their own).
- Cyber espionage (hacking into government or business data).
- Copyright infringement.

- Online gambling, or the illegal sale of goods.
- Solicitation, creation, or possession of child pornography.

Cyber crime includes either one of the following two elements:

- Criminal activity utilizing malware and viruses to target computers
- Using computers to commit other crimes

The following discusses a few cyber crimes related to [28]:

- **Computers as a Target:** These cyber crimes target computers, networks, or other electronic equipment. Technically knowledgeable cyber criminals carry out such cyber crime. By focusing on a computer, an attacker seeks to gain unauthorized access, damage it, or use it as a decoy for additional attacks. Computer systems can be compromised by viruses and malicious code.
- **Computer as Tool:** A computer could support online criminal activity. The main objective is to target a specific person rather than a system. The adversary takes advantage of human weaknesses through spam, phishing, scams, theft, and other illegal or offensive activities.
- **Cyber warfare:** Politically motivated attackers cause cyber warfare. These types of cyber crimes, also known as cyber war, are encouraged by the Internet and typically target financial and organizational systems by sabotaging their websites or engaging in sophisticated espionage.
- **Cyber terrorism:** Attackers with political motivations can also target computers, information systems, data, and programs. These attacks typically lead to conflict between various groups. They could be brought on by advanced persistent threats (APT), malware, viruses, worms, DoS attacks, phishing, and hacking methods.

15.3.2 NEED FOR BLOCKCHAIN SECURITY

By using blockchain technology and sharing data, transparency is possible. The involved parties are assured that the data they are working with is error free and unchangeable. This feature is useful not only in the technical field but also in other contexts. Here are a few factors contributing to blockchain technology's popularity across many industries [28]:

- **Transparency is guaranteed.** As an open-source technology, blockchain technology cannot be modified by other users. Blockchain technology is relatively secure because the logged data is challenging to alter.
- **It significantly lowers transaction costs.** Peer-to-peer and commercial transactions can be finished on a blockchain without the involvement of a third party. The transaction is completed more quickly because no intermediaries are involved.
- **Transaction settlements using blockchain technology are faster.** This is compared to traditional banks, which depend on operating hours and

protocols and whose locations around the world also prolong the delay. Blockchain, however, is devoid of these limitations, enabling quicker transaction settlement.

- **The lack of a central data hub encourages decentralization.** This enables the authentication of specific transactions. Even if the information is intercepted by adversaries while being updated on various servers, only a small amount of data will be compromised [29].
- **Users and developers take the lead in the transactions.** Third parties are no longer involved, introducing user-controlled networks.
- **Investigations are made simple.** When irregularities are found, carrying out the necessary actions can always be traced back to their source. Quality control follows from this.
- **Human error is eliminated.** Data is recorded and protected from manipulation using blockchain technology. Accuracy is ensured because records are examined every time they move from one node to another. Accountability ultimately results from this.
- **Complex and intelligent contracts can be easily verified, signed, and enforced.** This is with the help of blockchain technology.
- **Voting is made clearer.** Blockchain technology eliminates electoral fraud.
- **It is possible to track energy supply precisely.** Stock exchanges are thinking about the trustworthiness of blockchain technology.
- **Global peer-to-peer transactions are promoted.** Blockchain technology Make transactions involving cryptocurrencies quick, safe, and inexpensive.
- **Data is objective.** Blockchain technology protects data integrity and can notify users when data is changed. A balance is kept between security and governance so that, even if data for an organization is compromised, it cannot be used.
- **Devices are authenticated.** In blockchain technology, passwords could soon be replaced, eliminating the need for human intervention. This is because it does not support centralized architecture.
- **Non-repudiation.** Every transaction is digitally timestamped and signed. The history log continues to store earlier records even with the system's new iteration. Traceability results from this.

15.4 BLOCKCHAIN TECHNOLOGY: A SOLUTION FOR CYBER CRIMES

Most of the time, we can now understand, analyze, and make better predictions about criminal behavior before it occurs, thanks to blockchain technology. There is now a demand for a private security system that utilizes blockchain/distributed public ledger technology, according to the solution that several federal agencies have found to combat this issue.

Money laundering [17] is thought to be involved in 5% of all global GDP transactions, so the issue is only getting worse. Every year, illicit flows totaled close to \$1 trillion. Blockchain is used in this scenario to monitor money laundering transactions

and track them. Data is safe and secure and is guarded against hacking thanks to blockchain security.

Because cyber crime is the most worrying factor and cannot be solved immediately, blockchain technology is helping federal agencies stop these crimes against people and society. Major corporations and the financial sector are frequently the targets of hacker groups looking to steal money and data. A recent report [30] states, “An account belonging to the Bangladesh Bank, the country’s central bank, was hacked, resulting in a theft of \$81 million that was being held with the Federal Reserve.”

Recently, several institutions, such as Netflix and Twitter, have faced multiple data breaches. This includes incidents like the WannaCry ransomware attack and significant events such as the \$81 million theft from Bangladesh Bank. To stop these serious attacks against the nation’s economy, blockchain is a better option to stop these kinds of activities because it assists agencies with monitoring.

The European Union supported a project with a budget of about €5 million to prevent hackers and criminals from abusing blockchain technology. This “three-year project” is called Tools for Investigating Transactions in Underground Markets and involves 15 members working together. Interpol and other law enforcement organizations are involved in the project, which aims to create tools for disclosing traits typical of criminal transactions [31].

Banks are currently developing their fraud prevention system based on distributed ledger technology (also known as blockchain technology), which has multiple databases and helps to prevent cyber attacks. Today’s banking companies and other business institutions take cyber threats and attacks seriously. As a result, they have begun researching hybrid systems that can operate on the local, regional, and global levels [32].

Unlike blockchain, the first type of system protects legitimate customers’ privacy by keeping a personal record of all previous transactions while avoiding disclosing the specifics of each transaction. Afterward, the system must update and store all verified receivers, senders, and authenticated credentials. This kind of risk management system is in use by banks today to stop cyber attacks [33].

15.4.1 HOW AND WHY BLOCKCHAIN TECHNOLOGY PREVENTS CYBER CRIMES AND ATTACKS

- Blockchain technology has no single point of failure, greatly reducing the likelihood of an IP-based DDoS attack [34].
- Because blockchain technology is shared, it solves the problem of false consensus that the Byzantine Generals had [35].
- A platform that has been successful and hasn’t been the target of a cyber attack in seven years is Bitcoin. Data is saved/stored in every node, making hackers vulnerable and preventing them from carrying out a successful DDoS attack even if one or more nodes in the blockchain network are disrupted [36].

- Blockchain has operational resilience. Because the technology is distributed, any company using it for commercial or data security purposes can keep running and access its data even in the case of an attack on the blockchain network. The blockchain network is not completely secure. However, as we all know, there is a stage of the transaction request known as the “pending stage,” and during that pending state, it is possible for data to be falsified. A flaw was found in a 2014 attack on the Bitcoin network that was still in progress [37].

15.4.2 USING BLOCKCHAIN TECHNOLOGY TO PROTECT AGAINST CYBER ATTACKS

Blockchain technology can replace all data storage methods that serve as a record of property transfers, contracts, wills, and other legal documents. The development of cyber security requires the decentralization and distribution of all systems [38].

15.4.2.1 Blockchain in Anti-Money Laundering

By 2017, the global cost of anti-money laundering compliance will be nearly US\$8 billion. The use of blockchain in the struggle against money laundering is growing. If there is any informational gap during a transaction, regulators, law enforcement, and financial institutions like banks can now determine who the real and credentialed party is, greatly assisting regulators and allowing them to identify criminals quickly [39].

Hackers find it difficult to change the data in blockchain blocks and interfere in any business transaction. Therefore, the ledger’s data helps create formidable security and prevents crimes like money laundering, which fund terrorism and many other illegal activities.

15.4.2.2 Blockchain for IoT Security

Using primary private blockchains like Hyperledger Fabric, access control for network nodes (devices) is set up. This stops unauthorized access and securely keeps track of data control. It’s also used to make software installation safer by letting software updates be sent from peer to peer and by letting IoT devices be identified, validated, and sent securely. In the past, blockchain has been used to safeguard IoT sessions and connections and to spot malicious activity [39].

A security risk to the grid is that malware can be used to attack connected IoT devices. Therefore, botnet attacks have targeted IoT devices that launch DoS/DDoS cyber attacks. Smart doorbells, security cameras, and thermostats are a few examples [41]. More than ever, endpoint security measures must be effective, especially in light of the rise of mobile threats.

Today’s security perimeter is always changing and hard to define, so more than a centralized security solution is needed. Employees now connect to company networks using mobile devices, desktop computers, and laptops. Endpoint security strengthens centralized security by adding more security at the points of entry for many attacks and points of exit for sensitive data. Blockchain-based

data exchanges can be used to send secure data in almost real time and ensure that devices communicate with one another quickly. Because of its distributed nature and capacity for self-restoration via data validation nodes, the platform's blockchain-based architecture presents much greater difficulties for an attack [42, 43].

15.4.2.3 Blockchain in the Sharing and Storing of Data

To avoid a single point of failure in a storage ecosystem, using both public and private distributed ledgers is recommended. Hash lists make it simple to locate data that can be saved and stored safely, the Blockchain prevents unauthorized users from altering cloud data, and it is possible to verify the integrity of data sent between sender and receiver. In short, by using client-side encryption, which gives the actual data owners complete and verifiable control over their data, blockchain enhances the security of data sharing and storage.

15.4.2.4 Blockchain in Network Security

Many initiatives in this category focus on enhancing the authentication and secure storage of critical data in software defined networks (SDN) and containers. One approach involves utilizing a clustered structure of SDN controllers with a blockchain architecture to achieve these goals. Peer-to-peer (P2P) communication between network nodes and SDN controllers is made possible by the architecture, which uses private and public blockchains for network security.

15.4.2.5 Blockchain in Private User Data

The use of blockchain technology also addresses user privacy issues. To safeguard the information's confidentiality, mechanisms based on anonymization or encryption can be used [51]. Each node on a blockchain maintains a private share of data, limiting access to all data by all nodes. Then, without disclosing any information to other nodes, this node runs computations on that specific share. With such a setup, embedded devices require less memory, and data processing can be done more quickly, thanks to distributed storage.

Recent studies, however, have demonstrated how anonymized datasets can be de-anonymized [44]. Techniques for data anonymization are intended to safeguard personally identifiable information (PII). Thanks to blockchain technology, combining anonymization and decentralized data storage is possible. Internal and external attack surfaces could be minimized with the help of decentralized personal data management.

15.4.2.6 Blockchain in the Web and Navigation

Blockchain technology increases the dependability of wireless Internet access points by storing and tracking access control data on a local ledger. By using precise domain name system (DNS) records, the blockchain can also navigate to the appropriate web page. It can also be used to interact safely with online apps. These solutions involved using a consortium blockchain, in which a preselected set of network nodes manage the consensus process.

15.4.2.7 Blockchain in Phishing Emails

Phishing emails, which try to persuade recipients to click on a link, open a malicious file, or send email information to someone unaware of what is happening, are to blame for more than 90% of successful hacks and data breaches on critical infrastructure [48]. A decentralized blockchain-powered email system with built-in message authenticity could be advantageous for developing future smart grids. Blockchain-based emails could be used as an unchangeable transaction record to demonstrate an email's precise time and sender or recipient. This would improve the current nonrepudiation capabilities. Even if the blockchain is compromised, it isn't easy to alter the email records that are stored there [40].

15.4.2.8 Blockchain in Supply Chain Management Systems

The benefits of blockchain that are typically cited include traceability, transparency, and immutability, according to Chang and Chen [48]. They note that supply chains that have relied on conventional trust mechanisms based on centralized trust authorities may need help in accepting this idea. According to the authors, private (permissioned) blockchain may be better suited to a supply chain due to its higher degree of centralization as an entity with a clear boundary and constituency.

According to Pournader et al. [49], cyber security is one of the main problems that face international supply chains. They go on to say that the potential for blockchain to improve inventory/goods' traceability, transparency, and trust makes it relevant to supply chain management. They use IBM's blockchain to illustrate how identity management can be applied to cyber security. The results support that sharing important information safely and reliably is essential for a strong and effective supply chain.

In their discussion of challenges to blockchain adoption in supply chain cyber risk management, Etemadi, Van Gelder, et al. [50] note that this particular use-case of blockchain is still in its infancy. The technology's immaturity, lack of trust, and suitability are a few of the mentioned obstacles. They also discovered that a blockchain system's reliance on and need for trust in outside data sources, known as oracles, presents a significant challenge. According to the authors, blockchain is a decentralized database offering data security and transparency.

15.4.3 ISSUES, CHALLENGES, AND DIFFICULTIES OF USING BLOCKCHAIN TECHNOLOGY TO FIGHT CYBER CRIMES

In comparison to other technologies or methods currently in use for protecting relevant infrastructure, blockchain has profoundly impacted the world. Most people confuse blockchain with Bitcoin because, as was previously mentioned, it was first used in Bitcoin in 2008–2009 [46].

Be aware that Bitcoin is not a blockchain; rather, Bitcoin uses the concept of a blockchain (a cryptocurrency). Beyond cryptocurrencies, blockchain is currently used in many applications, including digital copies of your health and land records [45]. These records are saved digitally on the cloud using blockchain and are known

as smart contracts. No one can copy, alter, or pirate them. Blockchain has many benefits, but it also has many drawbacks. A few issues and difficulties must be overcome, and each briefly described next. Organizations/industries face these difficulties when attempting to solve common issues.

- **Cost:** The adoption of blockchain technology promises long-term benefits, but its initial implementation is expensive. Software organizations and industries need to integrate blockchain technology into their systems, which might have been classically developed for a particular organizational structure. This will drive up the cost, as opposed to being adopted or created independently. The organizational structure might also need specialized hardware to work with the software.
- **Lack of Skilled/Intelligent People:** In addition to dealing with the cost of the technology, operating it also requires a high level of intelligence. This problem worsens because there aren't enough engineers who can handle it, which causes organizations to have high demands for these engineers. According to most small or even medium-sized businesses, setting up a full or partial blockchain system is beyond their means because of the high setup costs.
- **Integration with Legacy System:** Organizations should try integrating with their current systems or fix their legacy systems as we move into the integration phase because setting up blockchain requires entirely different software. The system should be modified because implementing blockchain technology will initially be difficult to ensure a smooth transition. This process will also require significant human resources, including time, effort, and money. Due to the high cost of this technology, some businesses are hesitant to adopt blockchain solutions.
- **Energy Consumption:** Energy consumption is another difficult problem that must be considered [47]. It takes much energy to compute these difficult mathematical problems (including side-by-side verifying) for that network's secure transaction validation mechanism, which is complicated. Such massive energy use does not seem sustainable in a place where climate change is a major factor. Thus businesses are looking for more environmentally friendly business practices.
- **Lack of Public Awareness:** A lack of public awareness is another significant issue. The organizations using distributed ledger technology and the industries involved in this technology are dampening awareness of blockchain technology and its advantages. Therefore, raising public awareness is necessary before mainstreaming blockchain technology. Additionally, Bitcoin and blockchain are two distinct concepts, and people must understand their differences to utilize this technology fully.
- **Security:** Blockchain technology is created in a way that makes it accessible to the general public. The obvious need to protect the data and limit access poses serious problems for the government. Because of this, blockchain technology cannot be used where sensitive information is at stake.

15.5 CONCLUSIONS AND REMARKS

In this chapter, we have thoughtfully investigated and discussed blockchain networks and their security solutions as countermeasures against cyber criminals. Blockchain has been widely used to provide several security services, such as authentication, digital signature, and encipherment. Therefore, the development of blockchain-based resilience countermeasures tools and systems to defend users and systems against the exploitations of cyber criminals is in demand. Several state-of-the-art techniques were proposed in the literature to construct defense systems against cyber criminals/cyber crimes. Such systems mainly depended on either signature-based detection or anomaly-based detection. In this chapter, we shed light on the blockchain solutions for cyber criminals, concepts, elements, structure, and other aspects of blockchain utilization. Specifically, this chapter extended the elaboration on blockchain, blockchain components, blockchain architecture, its features, types, and limitations. Also, this chapter extended the elaboration on cyber criminals, their types, their security needs, blockchain solutions, as well as the issues, challenges, and difficulties of using blockchain technology to fight cyber crimes. This chapter deepened the knowledge of blockchain solutions for cyber criminals and provides more insight to readers about blockchain, cyber attacks, cyber criminals, and relevant countermeasures.

REFERENCES

1. Coin-desk (2023) *Crypto-Currency Market Capitalizations*. <https://coinmarketcap.com>
2. Al-Haija, Q.A., Alnabhan, M., Saleh, E. and Al-Omari, M. (2023 Jan. 1) Applications of Blockchain Technology for Improving Security in the Internet of Things (IoT). In *Blockchain Technology Solutions for the Security of Iot-Based Healthcare Systems* (pp. 199–221). Academic Press.
3. Peters, G.W., Panayi, E. and Chapelle, A. (2015) Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *arXiv pre-print arXiv:1508.04364*.
4. Foroglou, G. and Tsilidou, A.-L. (2015) Further Applications of the Blockchain. In *12th Student Conference on Managerial Science and Technology*, Athens University of Economics and Business, Athens, Greece, vol. 9.
5. Kosba, A., Miller, A., Shi, E., Wen, Z. and Papamanthou, C. (2016) Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Proceedings of IEEE Symposium on Security and Privacy (SP)*. San Jose, CA, IEEE, pp. 839–858.
6. Al-Haija, Q.A. and Alsulami, A.A. (2021). High Performance Classification Model to Identify Ransomware Payments for Heterogeneous Bitcoin Networks. *Electronics*, 10(17), 2113. <https://doi.org/10.3390/electronics10172113>
7. Zhang, Y. and Wen, J. (2015) An IoT Electric Business Model Based on the Bitcoin Protocol. In *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*. Paris, France, IEEE, pp. 184–191.
8. Albulayhi, K. and Al-Haija, Q.A. (2022, Dec 29) Security and Privacy Challenges in Blockchain Application. In *The Data-Driven Blockchain Ecosystem* (pp. 207–226). CRC Press.
9. Eyal, I. and Sirer, E.G. (2014) Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In *Proceedings of International Conference on Financial Cryptography and Data Security*. Berlin, Heidelberg, ACM, pp. 436–454.

10. Sharples, M. and Domingue, J. (2015) The Blockchain and Kudos: A Distributed System for the Educational Record, Reputation, and Reward. In *Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015)*. Lyon, France, Springer International Publishing, pp. 490–496.
11. Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System, *Decentralized Business Review* [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
12. Crosby, M., et al. (2016) Blockchain Technology: Beyond Bitcoin. *Applied Innovation*, 2(6–10), 71.
13. Raikwar, Mayank, et al. (2018) A Blockchain Framework for Insurance Processes. In *2018 9th IFIP International Conference on New Technologies, Mobility, and Security (NTMS)*. IEEE.
14. Ayoade, Gbadebo, et al. (2018) Decentralized IoT Data Management Using Blockchain and Trusted Execution Environment. In *2018 IEEE International Conference on Information Reuse and Integration (IRI)*. IEEE.
15. Ibrahim, R.F., Abu Al-Haija, Q. and Ahmad, A. (2022). DDoS Attack Prevention for Internet of Thing Devices Using Ethereum Blockchain Technology. *Sensors*, 22, 6806. <https://doi.org/10.3390/s22186806>
16. Mingxiao, Du, et al. (2017) A Review on Consensus Algorithm of Blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE.
17. Badawi, A. A. and Al-Haija, Q. A. (2021) Detection of Money Laundering in Bitcoin Transactions. In *4th Smart Cities Symposium (SCS 2021), Online Conference*. Bahrain, pp. 458–464. <https://doi.org/10.1049/icp.2022.0387>
18. Odeh, A., Keshta, I. and Al-Haija, Q.A. (2022). Analysis of Blockchain in the Healthcare Sector: Application and Issues. *Symmetry*, 14, 1760. <https://doi.org/10.3390/sym14091760>
19. NRI (2015) Survey on Blockchain Technologies and Related Services, *Technical Report*.
20. Johnson, D., Menezes, A. and Vanstone, S. (2001) The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1(1), 36–63.
21. Zheng, Z., et al. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14(4), 352–375.
22. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S. (2013) A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC'13)*. New York, ACM, pp. 127–140.
23. Biryukov, A., Khovratovich, D. and Pustogarov, I. (2014) Deanonymisation of Clients in Bitcoin p2p Network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. New York, ACM, pp. 15–29.
24. Eyal, I., Gencer, A.E., Sirer, E.G. and Van Renesse, R. (2016) Bitcoin-ng: A Scalable Blockchain Protocol. In *Proceedings of 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. Santa Clara, CA, Usenix, pp. 45–59.
25. Nayak, K., Kumar, S., Miller, A. and Shi, E. (2016) Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. In *Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroSandP)*. Saarbrücken, Germany, IEEE, pp. 305–320.
26. Billah, S. (2015) One Weird Trick to Stop Selfish Miners: Fresh Bitcoins, A Solution for the Honest Miner [Online]. Available: <https://eprint.iacr.org/2014/007>
27. Solat, S. and Potop-Butucaru, M. (2016) *ZeroBlock: Timestamp-Free Prevention of Block-Withholding Attack in Bitcoin, Technical Report*. Sorbonne Universities, UPMC University of Paris 6.

28. Priyadarshini, I. (2019) Introduction to Blockchain Technology. In *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies* (pp. 91–107). John Wiley & Sons.
29. Abu Al-Haija, Q., Al Badawi, A. and Bojja, G. R. (2022). Boost-Defence for Resilient IoT Networks: A Head-to-Toe Approach. *Expert Systems*, 39(10), e12934. <https://doi.org/10.1111/exsy.12934>
30. Law Enforcement Cyber Center. *Blockchain Consortium Seeks to Tackle Cyber Crime*. www.iacpccybercenter.org/news/blockchain-consortium-seeks-tackle-cyber-crime/. Accessed 20/Feb/2023.
31. Rebecca Campbell. Blockchain the Answer to Preventing Cyber Crime. *Cryptocoins News*. www.cryptocoinsnews.com/blockchain-cybercrime-prevention/. Accessed 25/Feb/2023.
32. Can Blockchain Prevent Cybercrime. *Distributed Ledger and Blockchain, Finextra*. www.finextra.com/blogposting/13032/can-blockchain-prevent-cybercrime. Accessed 25/Feb/2023.
33. <https://blog.ethereum.org/2016/09/22/transaction-spam-attack-next-steps/>. Accessed 25/Feb/2023.
34. <https://ice3x.co.za/byzantine-generals-problem/>. Accessed 23/Feb/2023.
35. <http://performermag.com/band-management/contracts-law/dot-blockchain-music-project/>. Accessed 23/Feb/2023.
36. Al-Haija, Q.A., McCurry, C.D. and Zein-Sabatto, S. (2021) Intelligent Self-reliant Cyber-Attacks Detection and Classification System for IoT Communication Using Deep Convolutional Neural Network. In Ghita, B., Shiaeles, S. (eds) *Selected Papers from the 12th International Networking Conference. INC 2020. Lecture Notes in Networks and Systems*, vol. 180. Springer. https://doi.org/10.1007/978-3-030-64758-2_8
37. Bryant Nelson. Blockchain Solution for Cyber & Data Security. *Richtopia*. <https://richtopia.com/emerging-technologies/blockchain-solutions-for-cyber-data-security>
38. Kyle Phillips. Blockchain: A New AML Kid on the Block. *Anti Money Laundering*. www.antimoneylaundering.lawyer/blockchain-anti-money-laundering/
39. Deshmukh, A., et al. (2022) Blockchain Enabled Cyber Security: A Comprehensive Survey. In *2022 International Conference on Computer Communication and Informatics (ICCCI)*. IEEE.
40. Huang, Z., Su, X. and Zhang, Y. (2016) A Decentralized Solution for IoT Data Trusted Exchange Based-On Blockchain. In *International Conference on Computing and Communication Technologies*, 2016. IEEE, Bikaner, India, pp. 1180–1184.
41. Basnet, S. and Shakya, S. (2018 May) BSS: Blockchain Security Over Software Defined Network. In *IEEE International Conference on Computing Communication and Automation*. IEEE, Greater Noida, India.
42. Makhdoom, A., Abolhasan, H.A. and Ni, W. (2019). Blockchain's Adoption in IoT: The Challenges, and a Way Forward. *Journal of Network and Computer Applications*, 125, 251–279.
43. Lee, R.M. (2017) Trisis: Analyzing Safety System Targeted Malware. *Dragos Blog*.
44. Shbair, Y. and Wallborn, A. (2018) A Blockchain-Based PKI Management Framework. In *IEEE NOMS Conference*. IEEE, Taipei, Taiwan.
45. Sawal, N.Y., Anjali, T., Amit, T., Sreenath, N. and Rekha, G. (2016) The Necessity of Blockchain for Building Trust in Today's Applications: An Useful Explanation from User's Perspective. Available at SSRN: <https://ssrn.com/abstract=3388558> or <http://dx.doi.org/10.2139/ssrn.3388558>
46. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A. and Felten, E. W. (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. In *2015 IEEE Symposium on Security and Privacy*. IEEE, SAN JOSE, CA, USA.

47. Abu Al-Haija, Q. and Al Badawi, A. (2022) High-Performance Intrusion Detection System for Networked UAVs via Deep Learning. *Neural Computing & Applications*, 34, 10885–10900. <https://doi.org/10.1007/s00521-022-07015-9>
48. Choo, K., Ozcan, S., Dehghantanha, A. and Parizi, R. (2020). Editorial: Blockchain Ecosystem-Technological and Management Opportunities and Challenges. *IEEE Transactions on Engineering Management*, 67(4). <https://doi.org/10.1109/TEM.2020.3023225>
49. Pournader, M., Yangyan, S., Seuring, S. and Koh, S. (2020). Blockchain Applications in Supply Chains, Transport, and Logistics: A Systematic Literature Review. *International Journal of Production Research*, 58(7), 2063–2081. <https://doi.org/10.1080/00207543.2019.1650976>
50. Etemadi, N., Van Gelder, P. and Strozzi, F. (2021). An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply III Chains Towards Cybersecurity. *Sustainability*, 13(9). <https://doi.org/10.3390/su13094672>
51. Al-Haija, Q. A. (2022) Time-Series Analysis of Cryptocurrency Price: Bitcoin as a Case Study. In *2022 International Conference on Electrical Engineering, Computer and Information Technology (ICEECIT)*. Jember, Indonesia, pp. 49–53, <https://doi.org/10.1109/ICEECIT55908.2022.10030536>

16 AI Classification Algorithms for Human Activities Recognition System With a Cyber Security Perspective

*Fahad Naveed, Shahbaz Ali Imran,
Aftab Alam Janisar, Aliyu Yusuf,
Salman Khan, and Inam Ullah Khan*

16.1 INTRODUCTION

The exponential growth of cyberspace use has resulted in the exponential growth of cyber criminal activities. As a result, cyber security has emerged as a major concern for both researchers and practitioners. This study uses a novel comparative methodology for recognizing human activity with the assistance of different calculations and picking the precise one. There are different strategies to perceive human activity recognition (HAR) from different sources; in this study, the research assures the accuracy of different calculations and then foresees the outcomes utilizing a few lattices like accuracy, precision, recall, and F-measure. Information collection is a significant step of the bend stepping stool. To record the actions and tests of subjects, subjects must have a smartphone or wear a smartwatch, outfitted with an accelerometer and gyroscope [1].

Analysts have distributed their datasets in this space. For this examination, this research utilizes the public dataset (Human Action Recognition Utilizing Smartphones), which is available on the UCI Machine Learning Repository [2]. For the dataset, a group of investigations were performed to gather data from 30 volunteers. The range of ages considered was 19–48. To record the signs, the Samsung Cosmic system SII was utilized. An aggregate of seven exercises were recorded: standing, standing, sitting, setting down, strolling, strolling to the ground floor, and strolling higher up. A solitary member performed these exercises twice. In the first session, there was a mount on the left half of the member. On the second attempt, the members were permitted to pace it as they were inclined. The analyses were conducted in research facility conditions; however, chips were approached to perform unreservedly the grouping of exercises for a more naturalistic dataset [3].

Six additional exercises were added during the preprocessing stage, which is flowing: stands to sit, sit to stand, sit to lie, lie to sit, stand to lie, lie to stand. The dataset is an assortment of information that compares at least one dataset of tables, in which each segment of the table shows a particular variable, and each line relates to the next and gives the record of the dataset. The dataset is an assortment of information that relates to at least one dataset table, in which each section of the table shows a particular variable, and each column compares to give a record of information [4]. Feature selection is utilized to refine information according to the features required [5]. The AI algorithm trains much more quickly on a larger data set, accuracy may be increased [6], overfitting may be lessened.

The decrease in complexity of feature selection is one of the focal points of artificial intelligence, which enormously impacts the performance of the model. Data on the features that you use to set up your simulated intelligence models will influence the display of the accomplishment. HAR frameworks utilize various techniques of simulated intelligence. The research deals with the informational index and comprehending which procedure is best for the proposed framework. The research contrasts the results by checking the precision of the applied algorithms. There are three feature selection techniques. K -NN is a sort of supervised machine learning algorithm. It is very basic but performs extremely complex group tasks. It is of non-parametric importance in that it doesn't expect anything about hidden data. It utilizes all the preparation data while characterizing another data point. It essentially computes the new data direct distance toward all the data points of preparation. At that point, it chooses the K -closest data point where K can be any whole number. Finally, it appoints the data highlight to the class to which most K data points belong. ANN is takes motivation from the human body. The force of decision making in it is 10^{-3} . Its cerebrum contains semiconductors, which make decisions. The human mind has around 10^{12} neurons and settles on decisions in 1 ms, yet semiconductors settle on decisions in nanoseconds. The pre-handling in it consists of info, activity function, yield.

SVM has become a cutting-edge classification strategy in statistical machine learning. The fundamental working rule of SVM is to find a hyperplane that isolates double-classed information with maximum margin. It cannot manage multiclass classification straightforwardly. The multiclass classification issue is typically tackled by the disintegration of the issue into a few two-class problems. This has become the cutting-edge classification technique in statistical machine learning [7].

16.2 LITERATURE REVIEW

This section presents an overview of existing literature on machine learning classification algorithms and cyber security.

16.2.1 CYBER SECURITY THREATS AND ATTACKS

As stated in the research [8], countries such as the United States, the UK, and 70 other nations have introduced the threat to intelligence frameworks and information security documents, describing national security issues [9]. These frameworks

TABLE 16.1
Important Terminologies

Term	Definition
Cyber security	“[T]he protection of data within a system against unauthorized disclosure, destruction, or modification, as well as the security of the system itself.”
Cyber space	A worldwide field in the information world that uses the electronic and electromagnetic spectrum to create, update, store, share, and use information through interconnected and dependent networks using new information and communication technology.
Vulnerabilities	Flaws in either the design or implementation of a system that make it possible for an attacker to carry out malicious commands, gain unauthorized access to information, and/or execute a variety of denial of service attacks.
Threats	Actions taken to benefit from security vulnerabilities in a system while simultaneously having a negative impact on the system.
Attacks	Exploitation is the process of finding weaknesses in a system and using a variety of tools and methods to find and exploit those weaknesses in order to cause damage to the system or to interfere with its normal operation. These attackers do so in order to achieve the harmful goals they have set for themselves, whether out of a desire for personal satisfaction or for financial gain.

Source: [13, 14].

are used to gather data from several sources and is evaluated by security experts. Nowadays, to analyze the threats, new techniques of machine learning are employed [10]. Hence cyber security is defined in a way that helps to prevent security attacks, enhance risk management, and avoid data breaches [11, 12].

Table 16.1 gives the definitions of key terms necessary for gaining a deeper understanding of the key concepts associated with this research topic.

In businesses, ensuring security is a key task. We can see two trends that are increasing the likelihood of security issues. For starters, as digitization progresses, the variety of assets involved in working settings expands rapidly. Second, attackers are becoming more adept in their methods of obtaining private information than in the past [15]. As a result, it is critical to have a thorough grasp of the security dangers that expose information systems and assets. Many worldwide security standards, such as NIST and ISO/IEC, are available to provide direction for dealing with security issues safely. In this context, there have been varied interests in security threat classification to develop countermeasures to address security hazards [16].

Antivirus software, firewalls, anti-pattern detection methods, and security protocols are just some of the open-source and commercial software solutions that help strengthen cyber security by protecting the IoT infrastructure from common cyber attacks. Current methods for detecting IoT attacks and malware are often proposed for specific applications—such as intrusion detection [17], malicious traffic detection [3], anomaly detection [18], and botnet detection [19]—using a wide range of AI techniques, including deep learning (DL), cyber threat intelligence (CTI), and deep neural networks (DNNs). The community has proposed a large number of

studies and related datasets for IoT cyber security [2, 19]. Several critical vulnerabilities have been reported in numerous surveys and studies that are specific to each tier of an IoT system and network. Because of their low power, memory, and computing capabilities, suitable cyber security remedies for IoT devices have yet to be well established.

Several papers have been published in the area of HAR methods M.S. Ryoo et. al [4] that the author used to check activities from visuals (e.g., videos). The relationship between different activities and structure is based on similarities that measure the spatiotemporal features. We used a scale invariant localization algorithm for checking multi-occurrences of these activities and detected them via an experiment by using our dataset. We are pleased to propose and confirm that our system can recognize complex human activities hierarchically.

16.2.2 LITERATURE BASED ON ML

In Jorge-L. et. al [20], TAHAR design was used for the recognition of physical exercises proposed by the author. An AI calculation for activity forecast and a sequential filter, which is used for refinement of yield, consolidated inertial sensors for catching body movement.

We checked its effective use on three human activities datasets that were gathered from assorted exercises, sensors and members, and the execution of beats from past related work recognition. The results demonstrated that recognition enhancements can be made to the framework when data is fluctuating in forecast exercises. This was done in the activity filtering module Tilt, which improves AI calculation (SVM) by the non-synchronous event of exercises by the relationships between bordering occasions. HAR alternatives designed have two executions.

In D. Angelita et. al [8], the placement of the sensors on the human body can become troublesome for the wearer and has the limitation that it cannot be used outdoors or in everyday life. Several machine learning models have been used to classify different activities. Two factors evaluate activity recognition methods: accuracy and computational cost. To reduce the computational cost, a method has been proposed to a build a multiclass support vector machine using integer parameters.

The authors' [9] examination presents a hybrid feature determination of model-based smartwatch sensor information, which vigorously recognizes different human exercises. The information is accumulated from inertial sensors (accelerometer and gyroscope) mounted on the midriff of the articles, i.e., people. Different exercises by people were recorded by analysts in an examination lab. An aggregate of 23 base highlights was applied to the dataset. A sum of 138 heterogeneous highlights were separated from the sensors. In any case, as a general guideline, a few out of every odd component contributed similarly to action acknowledgment; superfluous highlights corrupted the exhibition of the classifier. Hence the proposed crossover includes a choice strategy containing the filter and covering approaches and has assumed a significant role in choosing ideal highlights. Eventually, the chosen highlights were utilized for approval tests utilizing the SVM to distinguish human exercises. The proposed framework shows 96.81% normal classification execution utilizing ideal features, which is around 6% higher improved execution than with no component choice. The proposed model beats other cutting-edge models.

A. Tychkov et al. [7] presented new mathematics and approaches for EEG processing that help us find solutions that are fast and accurate, including increased emotional state conditions results. EEG processing made easy use of EMD method to show the change of the amount of IMFs received in a regular manner at EEG sections against the appearance of mental disorders for first and second leads.

M. Wang et al. [9] studied model reconfigurability incorporation in the layered convolutional neural network (CNN) via a deep structured model. It handles 3D activity recognition challenges well and enables us to do recognition rather than relying on handcrafted features but with raw RGB-D data.

Z. Shen et al. [10], for the first time, developed a pervasive fall detection system utilizing mobile phones as a platform. Experimental results of their prototype system name Preferred were excellent in terms of performance and power efficiency [11].

Elif Surer et al. [12] employed a video game that targets the CBRNE (chemical biological radiological neural explosion) domain, which is a scenario-based video game. This game version uses linear scenarios that join activities according to their project. The testing was done based on effectiveness by comparing it with two serious games, which were already there and created by game developers.

Ming Zeng et al. [21] proposed a CNN-based component extraction approach, which separates the nearby reliance and scale-invariant attributes of the increasing speed time arrangement. The trial results have demonstrated that, by extricating these qualities, the CNN-based methodology approached the cutting-edge level. Further improvement may be achieved by using unsupervised retraining and repeating the operations in multiple layers of the CNN model. This approach performs poorly when data from different users is considered. Feature extraction is one of the key measures in activity recognition because it can obtain relevant information to distinguish among various activities. Convolutional neural networks (CNN) have been employed for feature extraction in HAR.

M. Leo et al. [15] proposed classification results that are extremely promising. However, it is hard to recognize them as human beings, unless further recognition of items conveyed by the individuals are added to the framework. Future work is needed to manage these issues.

N. Feng and M. Abdel-Mottaleb [22] have proposed a calculation for activity division and recognition from video cuts containing complex exercises. Both movement and shape highlights were utilized for human exercises. The exercises included strolling, plunking down, standing up, and wiring on a whiteboard. The outcomes indicated that their calculation is viable for sectioning and perceiving complex exercises independently of the review bearing.

Sourav et al. [16] proposed center observational commitments with respect to the smartwatch plan and generally to the field activity recognition. To start with, they methodically show and assess the benefits of the profound learning strategy for RBMs, featuring the breaking points of a model of a multifaceted nature that are conceivable with appropriate vitality and execution time execution.

Xinding Sun et al. [17] introduced a general technique for complex HAR. The probability of the watched movement parameters is figured dependent on a multivariate Gaussian probabilistic model. The fleeting difference in the probability is displayed utilizing Gee. Their underlying test outcomes containing exercises, for

example, sitting, finding a workable pace seat, and hand-to-hand fighting, appear to be very encouraging. The system proposed here can be fitted in an increasingly broad Bayesian system.

F. Caba Heilbron et al. [3] have proposed a strategy that has been researched in two unique settings of human activities. More work is expected to explore how this technique scales to various conditions. The examinations have been completed in successions that have roughly the equivalent spatial goals. Their starter tests show that scaling can be dealt with by renormalizing the movement field suitably; however, more examination is required.

J. Wang et al. [18] have presented a system that creates a transient activity proposition on untrimmed recordings. They showed that their strategy can produce an excellent proposition with respect to restriction and positioning. From the efficiency perspective, our proposed strategy had the option to produce recommendations multiple times more quickly than past methodologies, as it runs at 10 FPS. They additionally indicated that our proposition could serve a significant job in a start-to-finish activity location pipeline by improving its general execution on a huge-scale benchmark. For future work, they are keen on further improving the efficiency of their proposed technique by interleaving or joining the element extraction and proposition portrayal stages, which are now done autonomously.

F. Zhang et al. [6] presented, first, a profound and inert organized model utilizing the convolutional neural system; second, a bound-together definition incorporating the span edge regularization with the component learning; third, successful learning calculation iteratively streamlines the subactivity disintegration, the edge-based classifier, and the neural systems. They exhibited the down-to-earth relevance of our model by viably perceiving human exercises. Utilizing a profundity camera, analyses on the open datasets led to their recommending that our model convincingly beats other best-in-class strategies under a few testing situations.

Y. Yang et al. [19] conducted significant research on HAR, specifically design recognition and inescapable processing. An overview of the ongoing development in profound learning for sensor-based activity recognition will soon be needed. Contrasted with conventional design recognition strategies, profound learning diminishes reliance on human-made element extraction and executes better via naturally learning significant-level portrayals of the sensor information. They feature the ongoing advancement in three significant classes: sensor methodology, profound model, and application, and they condense and talk about the reviewed research in detail. Finally, a few difficulties and achievable arrangements are displayed for future research.

A. A. A. D. J. Newman [2] investigated HAR, specifically structure recognition and unpreventable handling. At the present time, the progressing advancement in significant learning gravitates toward sensor-based activity recognition. Differently from regular plan recognition systems, significant learning lessens the dependence on human-made component extraction and achieves better execution by means of normal learning significant-level depictions of the sensor data. The progressing headway is divided into three significant classes: sensor philosophy, significant model, and application. The authors consolidate and talk about the investigations to date in detail. Finally, a couple of troublesome issues and attainable game plans are shown for future research.

D. Garcia-Gonzalez [23] researched the exhibition of existing AI techniques utilized in remote detecting and found that sign example irregularity initiated by human exercises makes the detecting framework flimsy. Inspired by our ongoing examination of the Fresnel zone model, they proposed a diffraction-based detecting model to set up a quantitative connection between signal variety and target activity. We broke down the proposed model theoretically and applies this model to identify nine various exercises, including seven body exercises. We manufactured a proof-of-idea model to approve and benchmark our framework. The proposed model can be applied to numerous other exercises and can be additionally used to improve the exhibition of existing AI frameworks. For our future work, we mean to apply the proposed technique to perceive other fine-grained and coarse-grained day-by-day exercises. F. Attal et al. [24] notes that, although the adoption of smart devices in HAR is not new, a significant amount of work has been done in this discipline. A majority of the previous studies that utilized IMU for activity recognition have adopted the approach to place these sensors on different parts of the body. Data was collected using IMU carried on the user's right hip, wrist, upper arm, ankle, and leg.

T. Peterek et al. [25] supervised the classification techniques linear discriminant analysis, the random forest, and the K -nearest neighbor and compared them in terms of better performance and accuracy. C. A. Ronao et al. [26] has shown that a two-stage continuous hidden Markov classifier is capable of handling time series data acquired from IMU. A hybrid evolutionary algorithm has been proposed that carries out the stages of data segmentation, feature extraction, and classification. L. T. Nguyen et al. [27] have developed a unified deep sense framework for HAR. Deep sense integrates convolutional and recurrent neural networks to exploit different types of relationships in sensor inputs. The ongoing progression and improvement of PC electronic devices have prompted the selection of keen home detecting frameworks, animating the interest for related items and administrations.

S. Yao, S. Hu, et al. [28] discuss the machine learning (ML) field for the programmed acknowledgment of human conduct. In this work, profound distinctive learning (DL) models were figured out and proposed for grouping human exercises. Specifically, the long short-term memory (LSTM) was applied for displaying spatio-worldly arrangements obtained by savvy home sensors. Test results performed on the inside for cutting-edge studies in versatile framework datasets show that the proposed LSTM-based methodologies beat existing DL and ML strategies, giving better analyzed outcomes than the current writing.

M. S. Ryoo et al. [29] offered a nitty-gritty depiction of their strategy, which won the SHL challenge by most precisely foreseeing the exercises on an unlabeled dataset. It can thus be viewed as the reference AR technique for the SHL dataset and a decent beginning stage for comparable AR issues. The features of the technique are the perplexing pipeline that incorporates novel pre-handling steps (for example, organizing the framework revolution), the extensive list of capabilities, the unpredictable component choice strategy, and the novel neural system engineering for profound learning. We additionally introduced how to improve the vitality utilization of our technique by adjusting sensor settings to every action. The key commitment, notwithstanding, may be the breadth of the strategy, which gives bits of knowledge on the viability of various techniques on the SHL dataset and incomparable spaces.

J. Weston et al. [30] offered a strategy that won the SHL challenge by most precisely foreseeing the exercises on an unlabeled dataset. The features are a perplexing pipeline that incorporates novel pre-handling steps, the novel neural system engineering for profound learning, and an extensive list of capabilities. We are introducing the vitality utilization of our technique by using adjustments sensor setting to every action.

L. Heike Brock et al. [31] note that HAR utilizing wearables has opened new open doors. They present another HAR system and show its viability through critical execution enhancements accomplished beyond the cutting edge and its generalizability by assessments across four various benchmarks: (1) advanced activity portrayals by abusing inert relationships between sensor channels, (2) consolidated focus misfortune to mitigate managing intra-class varieties of exercises; and (3) expanded multichannel time arrangement information with misunderstanding for better speculation. They accept that our work have new chances to additionally investigate HAR utilizing wearables.

16.3 RESEARCH METHODOLOGY

This chapter discusses the research techniques in this area, which include data collection, development, and preprocessing, as well as the tokenization procedure [2, 20]. Figure 16.1 depicts our study technique.

16.3.1 DATASET

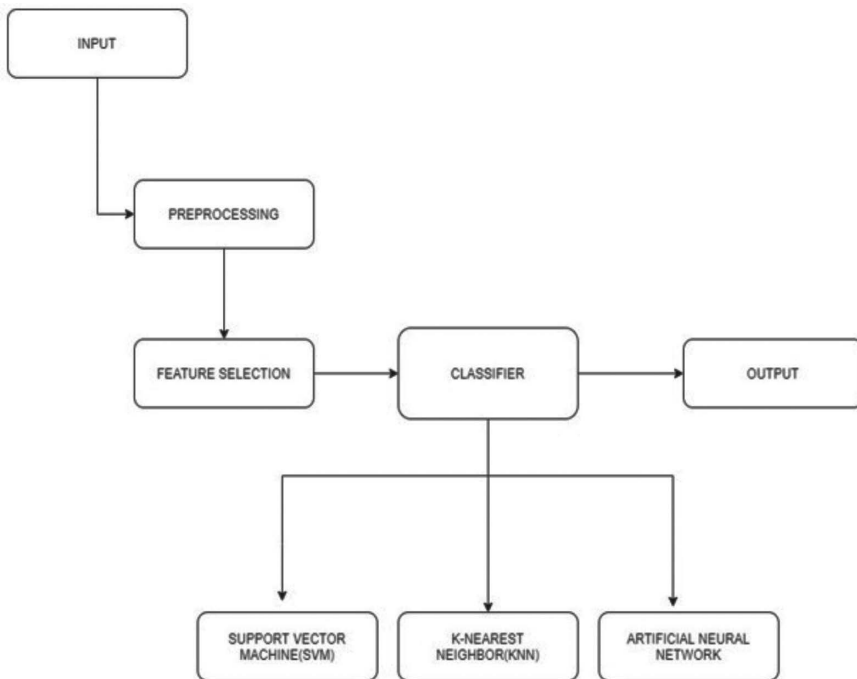


FIGURE 16.1 Dataset collection.

16.3.2 FEATURE EXTRACTION

Experiments are performed by the following.

Feature selection is utilized to refine information according to the features required, training the machine learning algorithm a lot more quickly, diminishing overfitting, giving better expectation power, and decreasing intricacy. Feature selection is one of the middle thoughts in AI, which enormously affects the presentation of the model. The data in the features are used to set up the AI models so as to influence the presentation to be achieved. HAR systems utilize various procedures of AI; it chips away at the informational index and arrives at which procedure is best for the proposed framework. Subsequent to applying various strategies, the results are contrasted by checking the precision of the applied algorithms.

The dataset was collected by the data from a sensor-based gyroscope/accelerometer. Data collection is a significant step on the ARC ladder. This progression requires a stage of protocol for recording the activity of tests of subjects carrying a cell phone or wearing a smartwatch that is outfitted with an accelerometer and gyrometer. Notwithstanding, a few researchers have distributed their datasets in this domain. For this investigation, we liked to utilize the free dataset (Human Activity Recognition Utilizing Cell Phones), which is available on UCI Machine learning Repository [2]. To gather this dataset, a group of trials were performed by a gathering 30 volunteers.

The base time of members was 19 to 48 years of age. To record the signs, a Samsung System SII was utilized. A total of six exercises were recorded standing, sitting, setting down, strolling, strolling downstairs, and strolling upstairs. These exercises were performed twice by a solitary member. In the first meeting, the PDA was mounted on the left half of the members. On the subsequent attempt, the members were permitted to place it as inclined. The investigations were directed in laboratory conditions; however, subjects were approached to perform a succession of exercises uninhibited for a more naturalistic dataset [3]. Six additional exercises were added during the preprocessing stage: stand to sit, sit to stand, sit to lie, lie to sit, stand to lie, lie to stand.

16.3.3 PREPROCESSING OF DATASET

Data can have loads of inconsistencies like missing qualities, blank sections, and incorrect data format, all of which needs to be cleaned. You need to measure, investigate, and condition data before displaying. The cleaner your data, the better your predictions will be. We additionally eliminated missing qualities and cleaned data to obtain the greatest exactness in this stage. Feature determination is a preprocessing step of a machine learning task.

- Filter method
- Wrapper method
- Embedded method

TABLE 16.2
Comparison of Filter, Wrapper, and Embedded Methods

Filter Methods	Wrapper Methods	Embedded Methods
Generic set of methods that do not incorporate a specific machine learning algorithm .	Evaluates on a specific machine learning algorithm to find optimal feature.	Embeds (fixes) features during the model building process . Feature selection is done by observing each iteration of model training phase.
Much faster compared to wrapper methods in terms of time complexity	High computation time for a dataset with many features	Sits between filter and wrapper methods in terms of time complexity.
Less prone to overfitting	High chances of overfitting because it involves training of machine learning models with different combination of features	Generally used to reduce overfitting by penalizing the coefficients of a model being too large.
Examples— Correlation, chi-square test, ANOVA, information gain , etc.	Examples— Forward selection, backward elimination, stepwise selection , etc.	Examples— LASSO, elastic net, ridge regression , etc.

Table 16.2 shows the comparison among the filters. Wrapper is utilized on subsets of features by assessing them by means of machine learning algorithms that employ systems of search to check through the space of subsets of potential features; every subset assessment is dependent on the quality and execution of the given algorithm. These methods additionally are known as voracious algorithms on the grounds that their motivation to track down the closest-to-ideal blend of features outcome in the best performing model, which will be costly with respect to computation and presumably illogical with respect to thorough inquiry.

The following are the three main techniques generally utilized for wrapper methods:

1. **Forward Selection:** Start with the null values, then check one by one every feature of data against significant value. It removes values with the same significant value and saves data having less value than the significant value.
2. **Backward Elimination Method:** This can start with all models (including all the independent variables), followed by the removal of the significant videos with less than f1 (F1 are the same features).
3. **Stepwise Selection:** This is similar to the forward selection method. The small difference is that a new feature is added. The significance checks feature is already added and add the finding-them feature and then simple remove the

unwanted data. Otherwise, save it. The embedded method is a combination of the filter and a wrapper methods that works just like a wrapper method.

16.3.4 CLASSIFIERS

The achievement speed of the classifier is expanded by utilizing a choice tree structure. The achievement speed of the classifier with K -NN rises with the choice tree k -NN calculation by utilizing the data of two sensors picked, as demonstrated in this work. As the achievement rate builds the choice tree, the design is applied to the SVM, ANN calculation.

- **k -Nearest Neighbor (K -NN):** In design recognition procedures, if the quantity of the class is expanded, the achievement of classifiers is getting significant. Also, the achievement speed of various frameworks shifts for each extraordinary smell. A characterization framework for n -butanol focuses has been pondered in this examination. Also, a calculation is proposed for multiclass issues with deficient data. Various features picked for each classifier in the choice tree structure are applied to the k -NN and SVM order algorithms. Also, the cross-approval procedure is used for expanding the achievement of order algorithms. The achievement speed of the classifier is expanded by utilizing a choice tree structure. The achievement speed of the classifier with K -NN rises with the choice tree k -NN calculation by utilizing the data of two sensors picked, as demonstrated in this work. Basically, as the achievement rate builds the choice tree, the design is applied to the SVM calculation.
- **Support Vector Machines (SVM):** SVM has evolved into one of the most advanced classification methods in statistical machine learning. SVM's core working premise is to find a hyperplane that separates binary classified data with the greatest possible margin. It cannot directly deal with multiclass classification. The multiclass classification problem is solved by dividing the problem into many two-class problems. For the multiclass classification with linear kernel, we employed the one-versus-one strategy (OVO). To evaluate the generalization capabilities of the classifier, we trained and tested it with a different division ratio of the training and testing dataset. We trained the SVM classifier with the ratio of 20:80% training and testing data, it showed pretty good results. The classifier was generalizing test samples with their accuracy. With a 70:30% division ratio of train and test data, it showed accuracy. Table 16.3 shows the results with different divisions.
- **Artificial Neuron Network (ANN):** To benefit from the neural network, we used tensorflow. As our data has 560 features, we used 560 neurons on our input layer. We used four hidden layers, each consisting of 50 neurons. The weights and biases are initialized with random values. Sigmoid is used as an activation function for each neuron. To find the loss, we used reduced mean along with cross entropy. To optimize the weights, we used Gradient Descent. Adam Optimizer was also tried, but it did not give more

than 16% accuracy. First, we conducted an experiment with a learning rate of 0.01, which is normally considered a good learning rate. The accuracy that we got was around 0.7, and the cost was just below 1. This showed that our optimizer was not working well with our learning rate. So we turned our learning rate and conducted an experiment with a learning rate of 0.5. By changing the learning rate, we achieved accuracy, and our cost also decreased to 0.17.

16.4 RESULTS AND DISCUSSION

This study combined the findings for each classifier with their individual features in precision, recall, and *F*-score for classical classifiers. The findings are shown in pie chart format, along with the metric score for the dataset of 560, in the following figures. Figure 16.2 displays the results for trained datasets, Figure 16.3 interprets the test dataset results, and Figure 16.4 depicts the dataset results of all features.

16.4.1 K-NN

K-NN is famous for refining data. We used this to get the best score upon fit and then to check its accuracy.

We checked the accuracy of 12 features against time to pass the preprocessed dataset to fit and train and then got the score by using the test data in the dataset. As

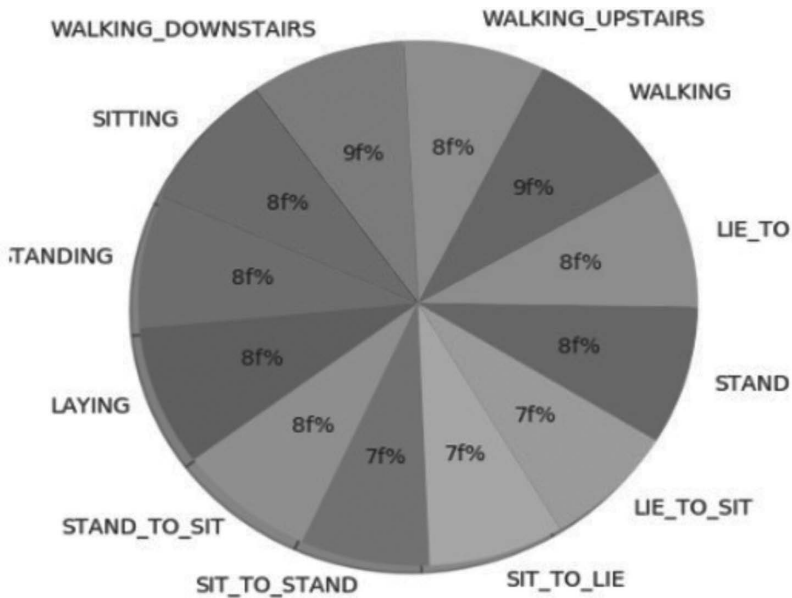


FIGURE 16.2 Train dataset results.

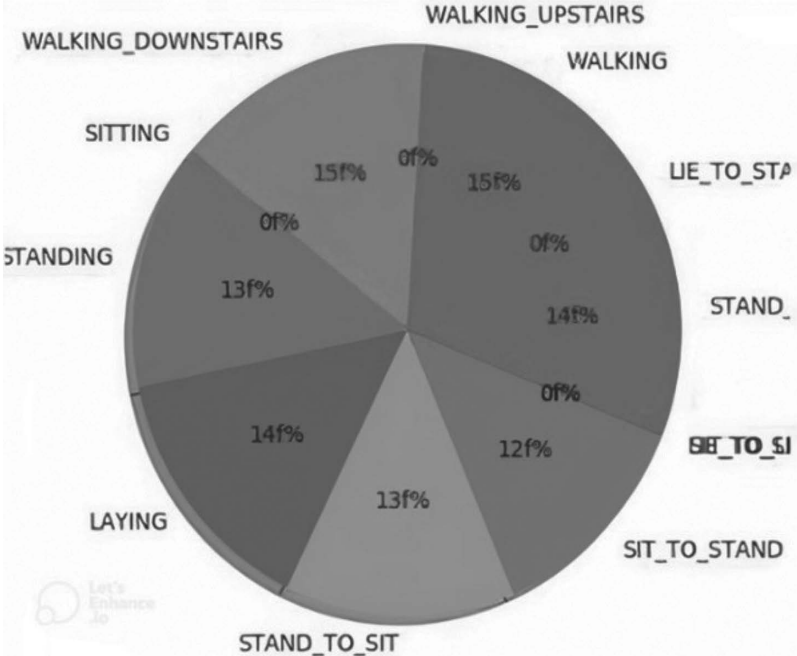


FIGURE 16.3 Test dataset results.

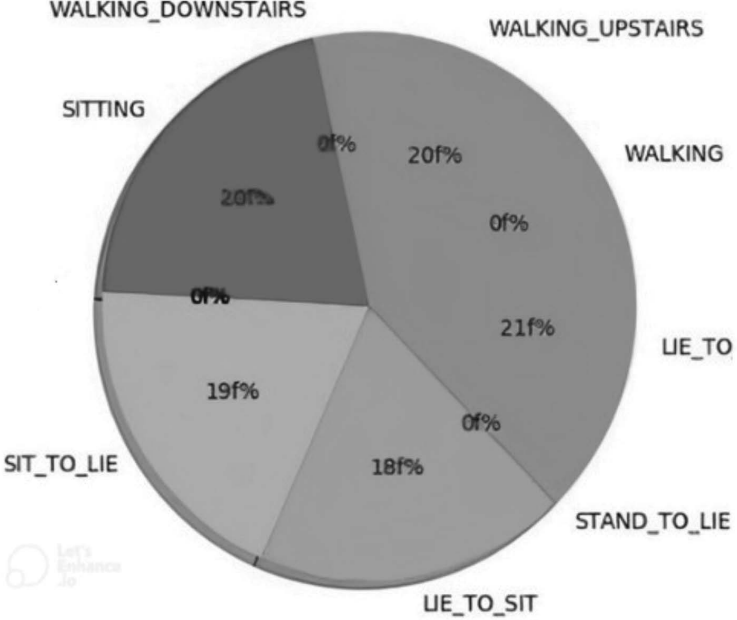


FIGURE 16.4 Dataset results of all features.

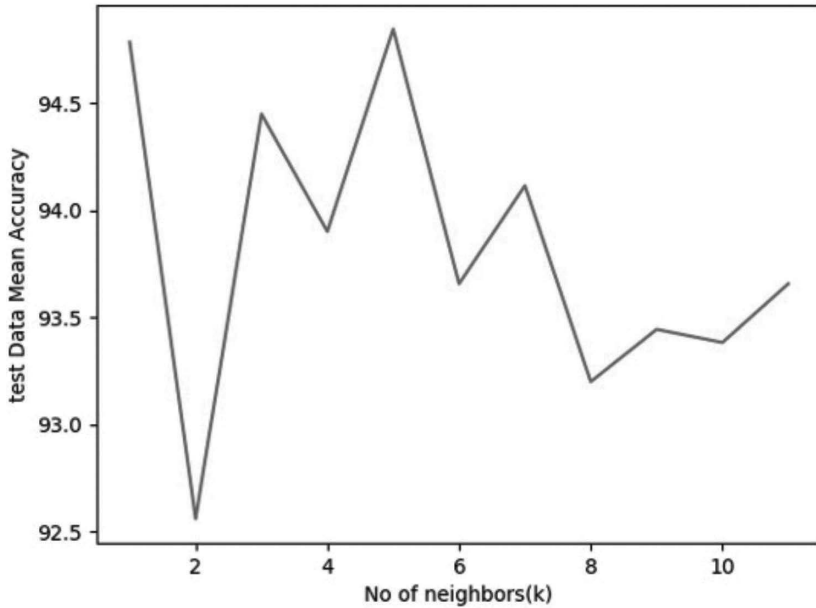


FIGURE 16.5 *K*-NN test dataset score.

in Figure 16.5 (code screenshot), we printed the accuracy of all features that we got by using this method. Table 16.4 displays the overall results of *K*-NN with respect to *F*-score iterations.

16.4.2 SVM USES MACHINE LEARNING TO SEPARATE DATA

Figure 16.6 interprets the test data confusion matrix of SVM. Table 16.3 displays the overall results of SVM with respect to *F*-score iterations.

16.4.3 ANN

ANN is used to train data. We used this to train data against the features, and then we created a 2D graph visualization of HAR, in which we get the different color representations of each activity to recognize them easily.

16.4.3.1 T-SNE Visualization of HAR

(*t*-SNE) *t*-distributed stochastic neighbor embedding is an unsupervised, nonlinear technique primarily used for data exploration and visualizing high-dimensional data displayed in Figure 16.7. In simpler terms, *t*-SNE gives you a feeling or intuition of how the data is arranged in a high-dimensional space. Figure 16.8 interprets the 3D visual representation of ANN result in a confusion matrix. Figure 16.9 is about the classification report of *F*-Score (decision tree).

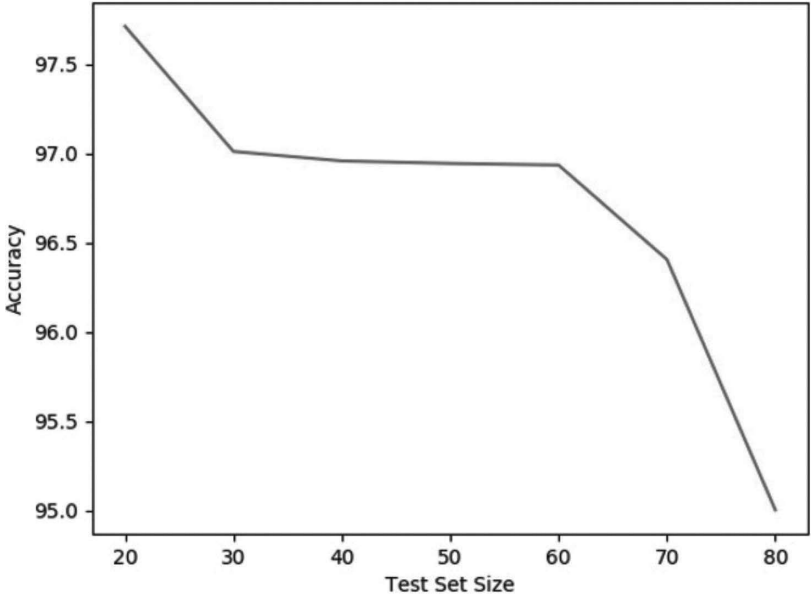


FIGURE 16.6 SVM test dataset score.

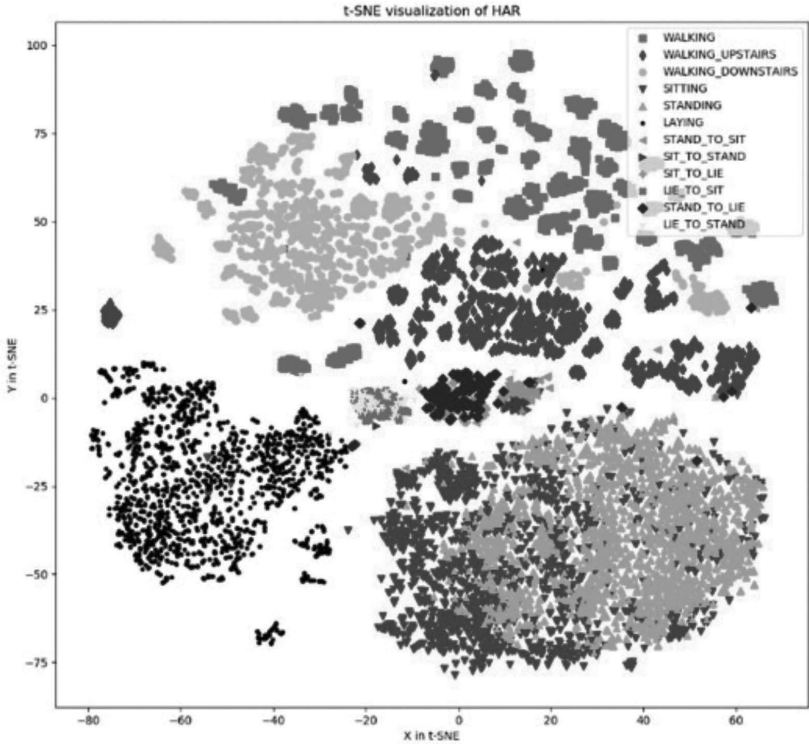


FIGURE 16.7 T-SNE visualization of HAR.

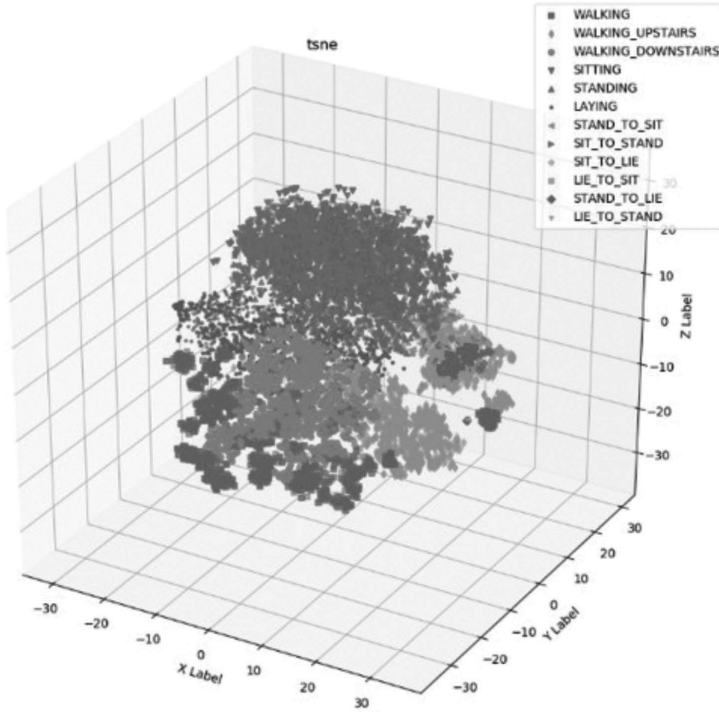


FIGURE 16.8 3D visual representation of ANN result: confusion matrix.

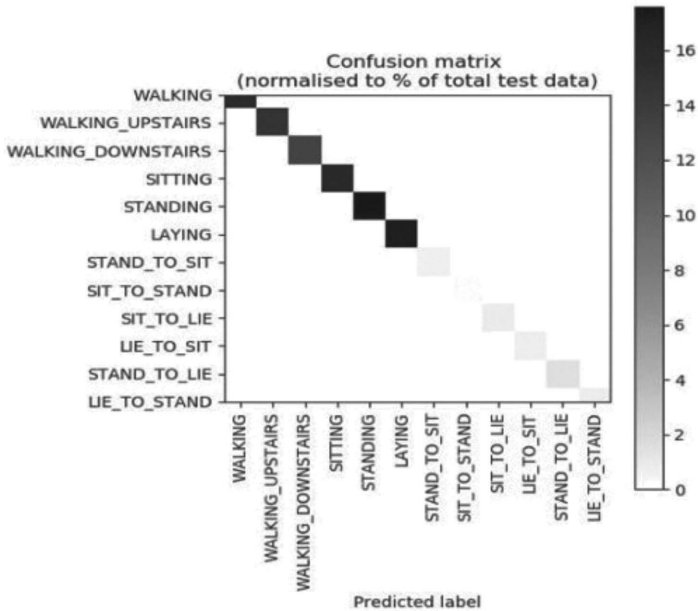


FIGURE 16.9 Test data confusion matrix of SVM.

16.4.3.2 Classification Report

	precision	recall	f1-score	support
WALKING	1.00	1.00	1.00	496
WALKING_UPSTAIRS	1.00	1.00	1.00	471
WALKING_DOWNSTAIRS	1.00	1.00	1.00	420
SITTING	1.00	1.00	1.00	508
STANDING	1.00	1.00	1.00	556
LAYING	1.00	1.00	1.00	545
STAND_TO_SIT	1.00	1.00	1.00	23
SIT_TO_STAND	1.00	1.00	1.00	10
SIT_TO_LIE	1.00	1.00	1.00	32
LIE_TO_SIT	1.00	1.00	1.00	25
STAND_TO_LIE	1.00	1.00	1.00	49
LIE_TO_STAND	1.00	1.00	1.00	27
accuracy			1.00	3162
macro avg	1.00	1.00	1.00	3162
weighted avg	1.00	1.00	1.00	3162

FIGURE 16.10 Classification report of F-Score (decision tree).

TABLE 16.3 SVM Results

Iterations SVM	F1-Score
01	0.970112
02	0.969579
03	0.969621

TABLE 16.4 K-NN Results

Iterations K-NN	F1-Score
01	94.784995
02	92.5587096
03	93.900579

16.5 CONCLUSION

In this chapter, the research used a dataset as input for preprocessing, and the second phase of research was feature selection based on processed data. The aim was to try to develop a system that will recognize the activity of humans by using/checking different recognition models with the help of sensors. Different techniques were used to develop a recognition system to build a HAR system; however, the research

introduced the method that utilizes the dataset to generate possible/precise outcomes with the classifiers SVM, naïve Bayes, decision tree, and K -NN Classifiers. The metric score for the dataset resulted in three multiple iterations for each classifier. In future, colony optimization can be utilized for recognition purposes [29]. This study was based on HAR systems, but in future, to address the security issues that threaten the cyber security environment, additional security measures are required to protect the cyber security environment from threats and other vulnerabilities using advanced machine learning mechanisms.

REFERENCES

- [1] N. Ahmed, J. I. Rafiq, and M. R. Islam, “Enhanced Human Activity Recognition Based on Smartphone Sensor Data Using Hybrid Feature Selection Model,” (in Eng), *Sensors (Basel)*, vol. 20, no. 1, 6 January 2020, <https://doi.org/10.3390/s20010317>.
- [2] A. A. A. D. J. Newman, “UCI Machine Learning Repository,” 2007 [Online]. Available: www.ics.uci.edu/~mllearn/MLRepository.html.
- [3] F. C. Heilbron, J. C. Niebles, and B. Ghanem, “Fast Temporal Activity Proposals for Efficient Detection of Human Actions in Untrimmed Videos,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 27–30 June 2016, pp. 1914–1923, <https://doi.org/10.1109/CVPR.2016.211>.
- [4] M. S. Ryoo and J. K. Aggarwal, “Spatio-Temporal Relationship Match: Video Structure Comparison for Recognition of Complex Human Activities,” in *2009 IEEE 12th International Conference on Computer Vision*, 29 September–2 October 2009, pp. 1593–1600, <https://doi.org/10.1109/ICCV.2009.5459361>.
- [5] R. Ding et al., “Empirical Study and Improvement on Deep Transfer Learning for Human Activity Recognition,” (in Eng), *Sensors (Basel)*, vol. 19, no. 1, 24 December 2018, <https://doi.org/10.3390/s19010057>.
- [6] F. Zhang et al., “Towards a Diffraction-based Sensing Approach on Human Activity Recognition,” in *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, pp. 1–25, 29 March 2019, <https://doi.org/10.1145/3314420>.
- [7] A. Y. Tychkov et al., “EEG Analysis Based on the Empirical Mode Decomposition for Detection of Mental Activity,” in *2017 IVth International Conference on Engineering and Telecommunication (EnT)*, 29–30 November 2017, pp. 130–134, <https://doi.org/10.1109/ICEnT.2017.35>.
- [8] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, “Human Activity Recognition on Smartphones Using a Multiclass Hardware-Friendly Support Vector Machine,” in *Ambient Assisted Living and Home Care*, J. Bravo, R. Hervás, and M. Rodríguez, Eds. Springer: Berlin, Heidelberg, 2012, pp. 216–223.
- [9] K. Wang, X. Wang, L. Lin, M. Wang, and W. Zuo, “3D Human Activity Recognition with Reconfigurable Convolutional Neural Networks,” in *Presented at the Proceedings of the 22nd ACM International Conference on Multimedia*, Orlando, FL, 2014 [Online], <https://doi.org/10.1145/2647868.2654912>.
- [10] J. Dai, X. Bai, Z. Yang, Z. Shen, and D. Xuan, “Mobile Phone-Based Pervasive Fall Detection,” *Personal and Ubiquitous Computing*, vol. 14, pp. 633–643, 1 October 2010, <https://doi.org/10.1007/s00779-010-0292-x>.
- [11] L. Wen, X. Li, L. Gao, and Y. Zhang, “A New Convolutional Neural Network Based Data-Driven Fault Diagnosis Method,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 7, pp. 1–1, 17 November 2017, <https://doi.org/10.1109/TIE.2017.2774777>.

- [12] S. Ariyurek, A. Betin-Can, and E. Surer, "Automated Video Game Testing Using Synthetic and Humanlike Agents," *IEEE Transactions on Games*, vol. 13, no. 1, pp. 50–67, 2021, <https://doi.org/10.1109/TG.2019.2947597>.
- [13] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171–3189, 2020.
- [14] N. R. Mosteanu, "Artificial Intelligence and Cyber Security—Face to Face with Cyber Attack—A Maltese Case of Risk Management Approach," *Ecoforum Journal*, vol. 9, no. 2, 2020.
- [15] M. Leo, T. D. Orazio, I. Gnoni, P. Spagnolo, and A. Distante, "Complex Human Activity Recognition for Monitoring Wide Outdoor Environments," in *Proceedings of the 17th International Conference on Pattern Recognition, 2004. ICPR 2004*, 26 August 2004, vol. 4, pp. 913–916, <https://doi.org/10.1109/ICPR.2004.1333921>.
- [16] V. Radu, N. D. Lane, S. Bhattacharya, C. Mascolo, M. K. Marina, and F. Kawsar, "Towards Multimodal Deep Learning for Activity Recognition on Mobile Devices," in *Presented at the Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, Heidelberg, Germany, 2016 [Online], <https://doi.org/10.1145/2968219.2971461>.
- [17] S. Xinding and B. S. Manjunath, "Panoramic Capturing and Recognition of Human Activity," in *Proceedings. International Conference on Image Processing*, 22–25 September 2002, vol. 2, pp. II–II, <https://doi.org/10.1109/ICIP.2002.1040075>.
- [18] J. Wang, Y. Chen, L. Hu, X. Peng, and P. S. Yu, "Stratified Transfer Learning for Cross-domain Activity Recognition," in *2018 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 19–23 March 2018, pp. 1–10, <https://doi.org/10.1109/PERCOM.2018.8444572>.
- [19] M. M. Yuhang Yang, and Baoxiang Liu, "Information Computing and Applications," *4th International Conference, ICICA 2013, Singapore, August 16–18, 2013. Revised Selected Papers, Part II*. Springer: Berlin, Heidelberg, vol. 392, 2013, <https://doi.org/10.1007/978-3-642-53703-5>.
- [20] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, *Human Activity Recognition on Smartphones Using a Multiclass Hardware-Friendly Support Vector Machine*, Ambient Assisted Living and Home Care, Springer, Berlin, Heidelberg, 2012, pp. 216–223.
- [21] M. Zeng et al., "Convolutional Neural Networks for Human Activity Recognition Using Mobile Sensors," in *6th International Conference on Mobile Computing, Applications and Services*, 6–7 November 2014, pp. 197–205, <https://doi.org/10.4108/icst.mobica.2014.257786>.
- [22] N. Feng and M. Abdel-Mottaleb, "HMM-Based Segmentation and Recognition of Human Activities from Video Sequences," in *2005 IEEE International Conference on Multimedia and Expo*, 6 July 2005, pp. 804–807, <https://doi.org/10.1109/ICME.2005.1521545>.
- [23] D. Garcia-Gonzalez, D. Rivero, E. Fernandez-Blanco, and M. R. Luaces, "A Public Domain Dataset for Real-Life Human Activity Recognition Using Smartphone Sensors," *Sensors*, vol. 20, no. 8, p. 2200, 2020 [Online]. Available: www.mdpi.com/1424-8220/20/8/2200.
- [24] F. Attal, S. Mohammed, M. Dedabrishvili, F. Chamroukhi, L. Oukhellou, and Y. Amirat, "Physical Human Activity Recognition Using Wearable Sensors," *Sensors*, vol. 15, pp. 31314–31338, 11 December 2015, <https://doi.org/10.3390/s151229858>.
- [25] T. Peterek, M. Penhaker, P. Gajdo, and P. Dohnalek, "Comparison of Classification Algorithms for Physical Activity Recognition," *Advances in Intelligent Systems and Computing*, vol. 237, pp. 123–131, 1 January 2014, https://doi.org/10.1007/978-3-319-01781-5_12.

- [26] C. A. Ronao and S. B. Cho, “Human Activity Recognition Using Smartphone Sensors with Two-Stage Continuous Hidden Markov Models,” in *2014 10th International Conference on Natural Computation (ICNC)*, 19–21 August 2014, pp. 681–686, <https://doi.org/10.1109/ICNC.2014.6975918>.
- [27] G. Hinton et al., “Deep neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups,” *IEEE Signal Processing Magazine*, vol. 29, no. 6, 2012, <https://doi.org/10.1109/MSP.2012.2205597>.
- [28] S. Yao, S. Hu, Y. Zhao, A. Zhang, and T. F. Abdelzaher, “DeepSense: A Unified Deep Learning Framework for Time-Series Mobile Sensing Data Processing,” *Proceedings of the 26th International Conference on World Wide Web*. ACM, Perth, Australia, 2017, <https://doi.org/10.1145/3038912.3052577>.
- [29] M. S. Ryoo, “Human Activity Prediction: Early Recognition of Ongoing Activities from Streaming Videos,” in *2011 International Conference on Computer Vision*, 6–13 November 2011, pp. 1036–1043, <https://doi.org/10.1109/ICCV.2011.6126349>.
- [30] J. Weston, S. Mukherjee, O. Chapelle, M. Pontil, T. Poggio, and V. Vapnik, “Feature Selection for SVMs,” *Advances in Neural Information Processing Systems*, vol. 13, pp. 668–674, 2000, ISBN. 9780262526517.
- [31] H. Brock, Y. Ohgi, and J. Lee, “Learning to Judge Like a Human: Convolutional Networks for Classification of Ski Jumping Errors,” in *Proceedings of the 2017 ACM International Symposium on Wearable Computers*, ACM, Maui, Hawaii, 2017, pp. 106–113, <https://doi.org/10.1145/3123021.3123038>.