IoT Enabled Multi-Energy Systems

From Isolated Energy Grids to Modern Interconnected Networks

Edited by
Mohammadreza Daneshvar
Behnam Mohammadi-Ivatloo
Kazem Zare
Amjad Anvari-Moghaddam

IoT Enabled Multi-Energy Systems

This page intentionally left blank

IoT Enabled Multi-Energy Systems

From Isolated Energy Grids to Modern Interconnected Networks

Edited by

Mohammadreza Daneshvar
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Behnam Mohammadi-Ivatloo
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Kazem Zare
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Amjad Anvari-Moghaddam
Department of Energy (AAU Energy), Aalborg University, Aalborg, Denmark

ACADEMIC PRESS
An imprint of Elsevier

Academic Press is an imprint of Elsevier
125 London Wall, London EC2Y 5AS, United Kingdom
525 B Street, Suite 1650, San Diego, CA 92101, United States
50 Hampshire Street, 5th Floor, Cambridge, MA 02139, United States
The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

ISBN: 978-0-323-95421-1

Publisher: Charlotte Cockle
Acquisitions Editor: Graham Nisbet
Editorial Project Manager: Teddy A. Lewis
Production Project Manager: Prasanna Kalyanaraman
Cover Designer: Victoria Pearson

Typeset by MPS Limited, Chennai, India

Contents

This page intentionally left blank

List of contributors

Amjad Anvari-Moghaddam Department of Energy (AAU Energy), Aalborg University, Aalborg, Denmark

Sasan Azad Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran; Electrical Networks Research Institute, Shahid Beheshti University, Tehran, Iran

Vandana Bassoo Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Mauritius, Réduit, Mauritius

Yogesh Beeharry Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Mauritius, Réduit, Mauritius

Arman Behnam Department of Computer Science, Illinois Institute of Technology, Chicago, United States

Nitish Chooramun Department of Software and Information Systems, Faculty of Information, Communication and Digital Technologies, University of Mauritius, Réduit, Mauritius

Mohammadreza Daneshvar Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Sobhan Dorahaki Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran

Jaber Fallah Ardashir Department of Electrical Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Mengzhu Gao Gotion Inc, Fremont, CA, United States

Saman Ghanbari Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

Mahdi Ghanbarzaad Khajeh Department of Electrical Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Mukesh Kumar Gupta Suresh Gyan Vihar University, Jaipur, Rajasthan, India

Mohammad Equebal Hussain Suresh Gyan Vihar University, Jaipur, Rajasthan, India

Rashid Hussain Moti Babu Institute of Technology, Forbesgunj, Bihar, India

David Jauernig Gotion Inc, Fremont, CA, United States

Trevor Jones Gotion Inc, Fremont, CA, United States

Mohsen Kalantar Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

Xiaojun Li Gotion Inc, Fremont, CA, United States

Mousa Marzband Electrical Power and Control Systems Research Group, Northumbria University, Newcastle upon Tyne, United Kingdom; Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah, Saudi Arabia

Sahar Mobasheri Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran

Behnam Mohammadi-Ivatloo Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Mojgan MollahassaniPour Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran

Masoud Rashidinejad Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran

Hadi Vatankhah Ghadim Department of Electrical Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Saeed Yadegari Department of Electrical Engineering, Razi University, Kermanshah, Iran

Preface

Nowadays, the energy grid in its diverse carriers is undergoing tremendous evolution due to rapidly appearing hybrid energy systems as well as stochastic devices in the core of the energy network infrastructure. Indeed, rapid developments in information technologies, different clean energy production systems, energy conversion units, and communication paradigms have driven the energy landscape to experience great changes. In such a hybrid energy structure, some crucial challenges threaten the reliable and sustainable operation of integrated energy networks due to the lack of cloud-based intelligent energy management and control systems, high level of stochastic fluctuations in the energy generation sector, and coordinated operation of different energy networks. In this respect, coordinated operation and energy management of multicarrier energy networks are essential for unbroken serving multi-energy demand, which needs cloud-based intelligent energy systems to realize secure connections among smart devices. In this regard, the Internet of Things (IoT) is recognized as a dominant solution for creating a cloud-based intelligent energy management scheme that enables hybrid energy networks for optimal cooperation. This book aims to evaluate the IoT-based solutions for facilitating the modernization process of multicarrier energy networks with a high/full share of renewables. It is targeted to cover the modeling, optimization, and assessing the necessity of IoT technologies and their applications for grid modernization, and coordinated operation of multivector energy grids, for an audience of energy, power, mechanical, chemical, process, and environmental engineers as well as the researchers and postgraduate students who work in the field of various types of energy systems. Indeed, this book scrutinizes the IoT-based solutions for optimally integrating multicarrier energy networks with a high/full contribution of renewable energy resources.

The current book consists of nine chapters. Chapter 1 wants to provide an overview of the key role of IoT in the energy management of future modern energy networks with a high/full share of renewable energy sources. Moreover, this chapter discusses the capability of IoT technology in improving synergies among the different smart energy management devices. Chapter 2 provides an overview of multi-energy interconnected systems in different energy grids. It also elucidates the role of interconnected multi-energy systems (MESs) in a smart city as a transactive energy structure and investigates the challenges and opportunities of interconnected MESs, as well as contests of IoT-based systems components and different control approaches. Chapter 3 aims to provide an overview of the application of IoT technology in the power failure positioning service in the power system operation. It also discusses the presence of IoT in the monitoring section of cyber-physical

power systems by having a look at its definition, structure, advantages, challenges, and future development opportunities. Chapter 4 describes the architecture and applications of IoT in smart grids. It also assesses the consequences of IoT in distribution networks, smart cities, microgrids, and smart buildings at the distribution level. Chapter 5 explains the features of the energy internet as the IoT in energy grid output that are appropriate for grid performance evaluation. It also discusses IoT challenges in the smart grid along with the future research and development potentials aiming to provide a suitable overview for future trends. Chapter 6 describes data science leverage and big data's role in IoT energy systems. It also discusses the related tools and analytics with attention to data-driven decision-making in smart energy systems. Chapter 7 presents the battery cloud that collects measured battery data from electric vehicles and energy storage systems. It also explains the applications of advanced algorithms for improving battery performance. Chapter 8 describes federated learning and its applications in security and privacy together with a demonstration case involving the implementation of a simulated model of federated learning for enhancing the security of systems. Chapter 9 aims to evaluate, develop, and test a lightweight string-matching technique suitable for a smart IoT-based virtual wireless sensor network.

As any research achievement may not be free of gaps, the editors kindly welcome any suggestions and comments from the respectful readers for improving the quality of this work. The interested readers can share their valuable comments with the editors via m.r.daneshvar95@gmail.com.

Mohammadreza Daneshvar
Behnam Mohammadi-Ivatloo
Kazem Zare
Amjad Anvari-Moghaddam

Overview of Internet of Things-based multi-energy management of cleaner multi-energy mix

1

Mohammadreza Daneshvar and Behnam Mohammadi-Ivatloo
Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

Chapter Outline

1.1 Introduction

Recent progress in information and communication technologies forces the energy structure to be upgraded in accordance with the new changes in different sectors of the energy network. The energy generation sector has experienced evolutionary changes by promoting decentralized energy generation units, especially intermittent renewable energy sources (RESs) [1]. How the system deals with unexpected variations in energy production is a challenge that needs innovative technologies to address [2]. From another perspective, multi-energy devices create reliance among various energy networks and drive energy grids to be operated interdependently [3]. Now, such challenges make the energy management of the cleaner multi-energy mix structure difficult. Due to this, addressing the aforementioned challenge became the prominent goal of similar researches in recent works. In most of these studies, the Internet of Things (IoT) was the main tool that is used as an effective remedy for acquiring suitable outcomes. In Ref. [4], an IoT enabled novel method is presented for enhancing the network reliability as well as optimizing the operation costs considering the uncertainty effects in the energy management of the integrated energy system with multicarrier energy hubs, RESs, plug-in hybrid electric vehicles, and combined heat and power. In another work [5], the authors applied an advanced IoT technology for the energy management of an intelligent commercial building system. The proposed smart energy management framework is used for determining the most economic conditions for commercial buildings. An IoT-based framework is suggested in Ref. [6] for monitoring and measuring the distribution sector data with very low latency and higher controllability and

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00001-X

accuracy aiming to investigate the economic and social aspects of the distribution system with various types of RESs. In Ref. [7], the multiobjective distributed dispatching algorithm is used for introducing an IoT-based energy management system to facilitate the incorporation of green energy resources in the smart electrical grid. The IoT framework is used in Ref. [8] for proposing the energy management system with the aim of optimally controlling distribution system resources based on continuous data monitoring. In Ref. [9], a new IoT framework is proposed to benefit the effective potential of IoT in developing an energy-efficient intelligent lighting system with significant energy savings. Moreover, the development and design of the IoT-based domain model are assessed in Ref. [10] to provide a basic understanding of flexible energy management strategies for the effective energy exchange in the presence of RESs. According to the recent studies in the context of IoT, the idea of merging IoT-based technologies with intelligent energy systems together indicates immense growth potential and attracts the attention of the research community in grid modernization plans [11]. At the pinnacle of the grid modernization expansion stage, IoT-based technologies offer a promising way of implementing energy programs with high-quality energy services. The IoT-based technologies can reduce congestion and enhance energy efficiency for improving the reliability of energy supply and making the realization of 100% RESs possible for future modern energy networks. Given the key role of IoT-based technologies in successfully implementing grid modernization schemes, this chapter is targeted to provide an overview of their application in the multi-energy management of a cleaner multi-energy mix. To this end, this chapter discusses the real-world applications of IoT, its characteristics, opportunities, and challenges in the modern energy grid area.

1.2 Applications of Internet of Things

In the IoT paradigm, several smart objects can interact with each other and these interactions can be formed based on exchanging different types of information such as multimedia data and sensor data. In recent years, IoT penetration is highly increased in various sectors of the economy to improve the quality of life [12]. Its services can intelligently shape people's lives in different layers from agriculture to health care. Some of the real-world applications of IoT are depicted in Fig. 1.1 [13,14].

1.3 Characteristics of Internet of Things

With the ceaseless development of different technologies, there is an urgent growth in the need for multicarrier energy in the life cycles. This enormous requirement for a multi-energy supply demonstrates the necessity for new coordinated technologies to make the energy supply match its demand. Such revolutions in modernization can be realized with end-to-end IoT solutions. In today's world, manifold definitions are presented for IoT due to its rapidly growing applicability in multifarious research domains. Beyond giving specialized services for diverse goals, IoT

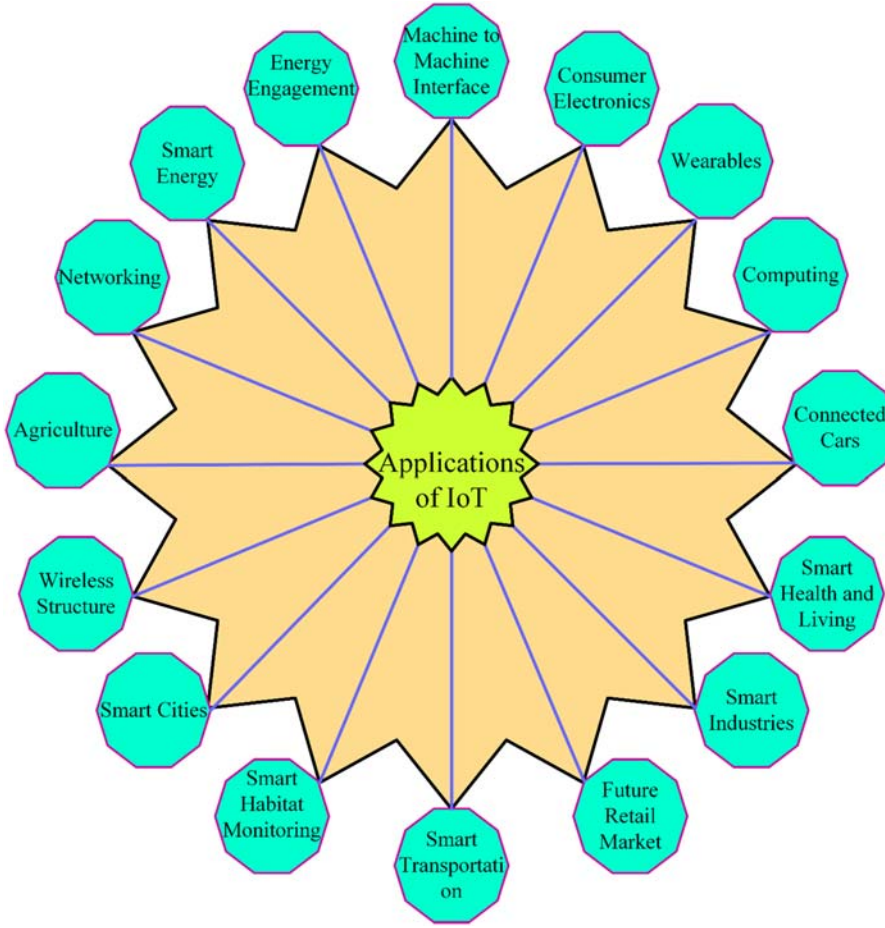


Figure 1.1 Real-world applications of IoT [13,14]. *IoT*, Internet of Things.

platforms have enough potential for flexibility in allowing third parties to use the application program interface for developing complex applications [15]. In this respect, the technology synthesis is essential for binding the work of automatics, artificial intelligence technology, advanced network technology, and perceptive technology together into a system possible aiming to establish the interconnection of objects and people [16]. The IoT-based technologies can facilitate the coordinated development of lifestyle and its culture, society, work, habitat, and material production environment according to the theory for the social−economic−natural complex ecosystem that is in line with the IoT purpose [17,18]. A large number of existing intelligent devices force the system to require interoperability throughout the different layers of the integrated system. This issue is immensely intensified by working under the IoT architecture with numerous technologies and smart devices. Fig. 1.2 exhibits the general characteristics of IoT in smart systems.

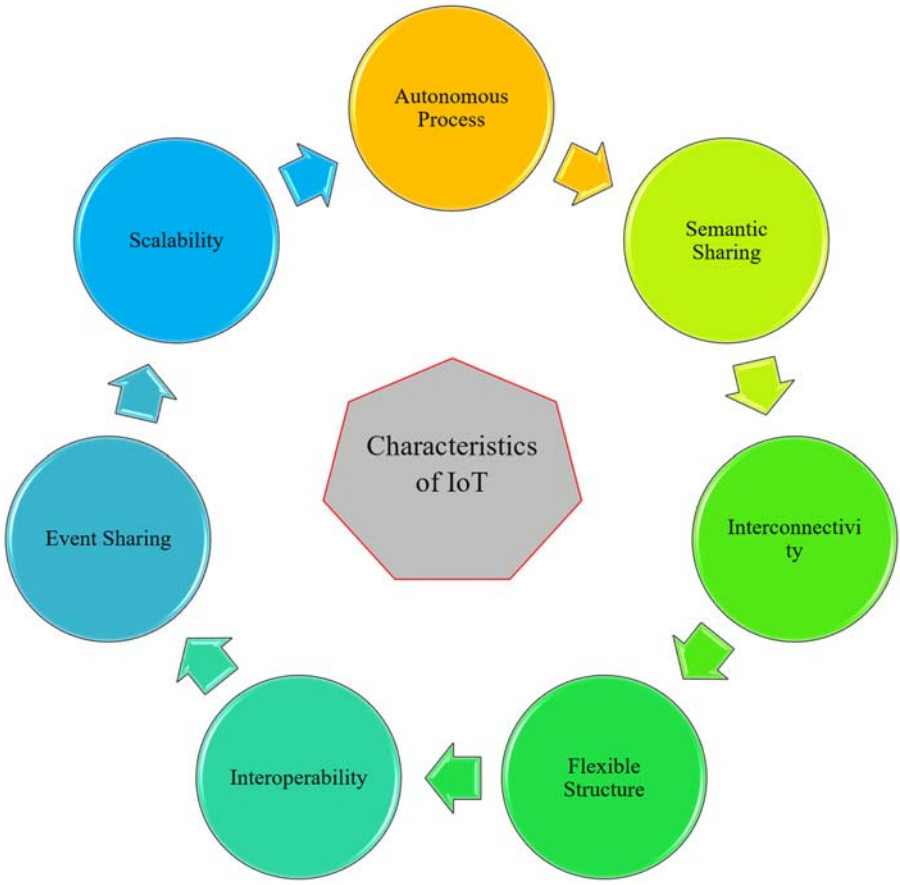


Figure 1.2 General characteristics of IoT in smart systems. *IoT*, Internet of Things.

The IoT architecture is the collection of enormous intelligent devices, which are interconnected and need to be coordinately worked under the integrated management umbrella. The success of the IoT's missions directly depends on the purposeful interoperability among smart devices. As all interactions pursue the autonomous process on a large scale, the scalability of adopted technologies is essential for the IoT platform. The data deluge and extensibility are other key characteristics of IoT that have important effects due to the generation of data all the time.

1.4 Opportunities of Internet of Things

IoT-based technologies offer plenty of benefits due to their ability to implement smart connections with high-quality services [19]. Such types of connections can bring the automation opportunity for the network of intelligent devices. Automation can

Figure 1.3 Some of the important opportunities of IoT [13]. *IoT*, Internet of Things.

provide the possibility of controlling different smart products leading to the management of the action of day-to-day activities as well as uniformity of tasks. Herein, a transparent process can be maintained under this automation over the entire machine-to-machine communication as one of the main advantages of automation. Automation, alongside the existence of a machine-to-machine interface, can increase the efficiency of the overall system. Thus increasing efficiency is another prominent opportunity for the modern energy network that can be reached using IoT-based technologies. IoT technologies realize such opportunities by developing communication platforms that create connectivity among devices on a daily basis resulting in the improvement of the quality of services and time factor. Such communications facilitate energy interactions among multifarious agents that arrange cost-effective day-to-day activities and make the system's development economical. Hence, IoT platforms procure cost-saving opportunities in various sectors of the modern grid.

On the other hand, the network of connected intelligent devices makes instant access to data possible in a rapid fashion. This is a great opportunity for simply managing the process and conducting decision-making very quickly, which helps in making the people's life easier and more comfortable. Fig. 1.3 illustrates some of the important opportunities created by IoT [13].

1.5 Challenges of Internet of Things

In recent decades, energy networks have witnessed momentous changes in their different forms from generation, transportation, and utilization around the world [20]. One of the key transformations is related to the increase of RESs' penetration, which brings uncertainties to the system scheduling [21]. Another one is the

massive emergence of smart devices in various parts of energy networks, which brings complexity and technological challenge to system management. As mentioned, IoT-based technologies are introduced as a promising way of the energy management of a cleaner multi-energy mix. Although IoT-based platforms are introduced as one of the effective remedies for addressing the mentioned concerns, their implementation and usage create new challenges for the modern energy grid that needs to be deeply analyzed and addressed. In the IoT enabled energy structure, dynamically connecting numerous appliances and services to each other [22] threaten privacy preservation by making the stored information readily available. Thus such information is open to hackers' attacks with unauthorized concerns [23], so the privacy and security issue is one of the main challenges of IoT. Another challenge is related to the compatibility issue due to the lack of sufficient international standards that can provide appropriate conditions for the stakeholders and manufacturers to have interactions with the services without difficulties. In the widespread network of connected smart devices, the complexity is another key concern as the occurrence of a small failure in the hardware and software components can result in damaging the entire system. In addition to the complexity, such networks rely on the machine-to-machine interface with the automation control and procedure that reduces the need for employees as well as human interactions in the process. Fig. 1.4 demonstrates some of the important challenges of IoT [13].

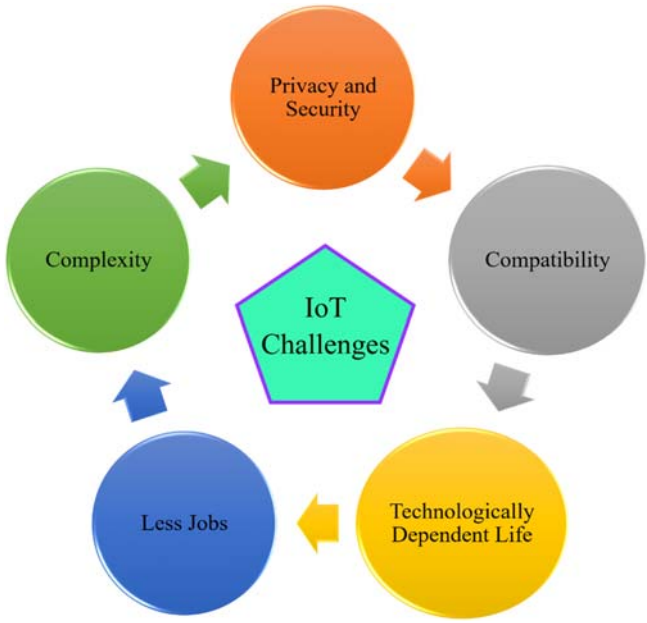


Figure 1.4 Some of the important challenges of IoT. *IoT*, Internet of Things.

1.6 Summary

A multitude of decentralized energy generation technologies, especially RESs, are on the verge of becoming the common alternative to traditional energy production units to effectively benefit economic and environmental advantages. Herein, clean energy systems are targeted for multi-energy generation, which brings up the need for the energy management of cleaner multi-energy mix processes. Meeting such requirements of modern energy networks cannot be possible without using IoT technologies for the automation control of the system. Due to this, the present chapter provided an overview of the IoT-based multi-energy management of a cleaner multi-energy mix. In this respect, the real-world applications of IoT were investigated to give a suitable overview regarding its capability for the energy control and management of future modern energy networks. The characteristics of IoT were scrutinized to clarify how IoT-based technologies can realize the comprehensive autonomous process with a high level of interoperability among a large number of connected intelligent devices. In the end, the opportunities and challenges of IoT were deeply investigated to highlight the strengths and weaknesses of IoT schemes in implementing the practice plans of future modern multi-energy networks. The conducted overview provides a clear understanding of IoT capability in the success of smart energy programs in facilitating the transition from isolated energy grids to modern interconnected energy networks.

References

[1] M. Daneshvar, B. Mohammadi-Ivatloo, M. Abapour, S. Asadi, Energy exchange control in multiple microgrids with transactive energy management, J. Mod. Power Syst. Clean. Energy 8 (4) (2020) 719−726.

[2] M. Daneshvar, B. Mohammadi-Ivatloo, K. Zare, S. Asadi, Transactive energy management for optimal scheduling of interconnected microgrids with hydrogen energy storage, Int. J. Hydrog. Energy 46 (30) (2021) 16267−16278.

[3] M. Daneshvar, B. Mohammadi-Ivatloo, K. Zare, M. Abapour, S. Asadi, A. Anvari-Moghaddam, Chance-constrained scheduling of hybrid microgrids under transactive energy control, Int. J. Energy Res. 45 (7) (2021) 10173−10190.

[4] B. Kazemi, A. Kavousi-Fard, M. Dabbaghjamanesh, M. Karimi, "IoT-enabled operation of multi energy hubs considering electric vehicles and demand response," *IEEE Transactions on Intelligent Transportation Systems*, IEEE, 2022.

[5] C. Liu, D. Wang, Y. Yin, Two-stage optimal economic scheduling for commercial building multi-energy system through internet of things, IEEE Access. 7 (2019) 174562−174572.

[6] S. Ding, J. Zeng, Z. Hu, Y. Yang, IOT-based social-economic management of distribution system with the high penetration of renewable energy sources, Sustain. Cities Soc. 76 (2022) 103439.

[7] Z. Xiaoyi, W. Dongling, Z. Yuming, K.B. Manokaran, A.B. Antony, IoT driven framework based efficient green energy management in smart cities using multi-objective distributed dispatching algorithm, Environ. Impact Assess. Rev. 88 (2021) 106567.

[8] P.R. Krishnan, J. Jacob, An IOT based efficient energy management in smart grid using DHOCSA technique, Sustain. Cities Soc. 79 (2022) 103727.
[9] Z. Chen, C. Sivaparthipan, B. Muthu, IoT based smart and intelligent smart city energy optimization, Sustain. Energy Technol. Assess. 49 (2022) 101724.
[10] C. Ziogou, S. Voutetakis, S. Papadopoulou, Energy management strategies for RES-enabled smart-grids empowered by an Internet of Things (IoT) architecture, Computer Aided Chemical Engineering, 40, Elsevier, 2017, pp. 2473−2478.
[11] M. Daneshvar, S. Asadi, CPS-based transactive energy technology for smart grids, Cyber-Physical Systems in the Built Environment, Springer, 2020, pp. 323−338.
[12] A. Mellit, S. Kalogirou, Artificial intelligence and internet of things to improve efficacy of diagnosis and remote sensing of solar photovoltaic systems: Challenges, recommendations and future directions, Renew. Sustain. Energy Rev. 143 (2021) 110889.
[13] S.S. Reka, T. Dragicevic, Future effectual role of energy delivery: a comprehensive review of Internet of Things and smart grid, Renew. Sustain. Energy Rev. 91 (2018) 90−108.
[14] F.K. Shaikh, S. Zeadally, E. Exposito, Enabling technologies for green internet of things, IEEE Syst. J. 11 (2) (2015) 983−994.
[15] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Computer Netw. 57 (10) (2013) 2266−2279.
[16] F. Tao, Y. Wang, Y. Zuo, H. Yang, M. Zhang, Internet of Things in product life-cycle energy management, J. Ind. Inf. Integr. 1 (2016) 26−39.
[17] S. Ma, R.S. Wang, "The social-economic-natural complex ecosystem,", Acta ecologica Sin. 4 (1) (1984) 1−9.
[18] W. Rui-gang, Main character and basic theory for Internet of Things, Computer Sci. 39 (6A) (2012) 201−206.
[19] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, J. Yan, 5G network-based Internet of Things for demand response in smart grid: a survey on application potential, Appl. Energy 257 (2020) 113972.
[20] M. Daneshvar, B. Mohammadi-Ivatloo, M. Abapour, S. Asadi, R. Khanjani, Distributionally robust chance-constrained transactive energy framework for coupled electrical and gas microgrids, IEEE Trans. Ind. Electron. 68 (1) (2020) 347−357.
[21] M. Daneshvar, H. Eskandari, A.B. Sirous, R. Esmaeilzadeh, A novel techno-economic risk-averse strategy for optimal scheduling of renewable-based industrial microgrid, Sustain. Cities Soc. 70 (2021) 102879.
[22] M. Ammar, G. Russello, B. Crispo, Internet of Things: a survey on the security of IoT frameworks, J. Inf. Security Appl. 38 (2018) 8−27.
[23] J. Lopez, R. Rios, F. Bao, G. Wang, Evolving privacy: from sensors to the Internet of Things, Future Gener. Computer Syst. 75 (2017) 46−57.

Overview of multi-energy interconnected systems in different energy grids

2

Sahar Mobasheri[1], *Sobhan Dorahaki*[1], *Masoud Rashidinejad*[1] *and Mojgan MollahassaniPour*[2]
[1]Department of Electrical Engineering, Shahid Bahonar University of Kerman, Kerman, Iran, [2]Faculty of Electrical and Computer Engineering, University of Sistan and Baluchestan, Zahedan, Iran

Chapter Outline

Abbreviations

CAES	compressed-air energy storage
CHP	combined heat and power
DRP	demand response program
IEA	international energy agency
IGDT	information gap decision theory
IoT	internet of things
MES	multi-energy system

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00002-1

MINLP mixed integer nonlinear programming
MILP mixed integer linear programming
PDF probability distribution function
PV photovoltaic
P2G power to gas
P2P peer to peer
TE transactive energy

2.1 Introduction

World energy consumption is projected to increase by 34% up to 2035 [1]. Moreover, it is predicted that electricity consumption will grow 48% between 2012 and 2040 [2]. The increasing use of energy leads to rise up more environmental and economic challenges, especially the climate change and the fossil fuels crises [3]. To deal with such concerns, a sustainable way of development is required focusing on energy productivity and distributed energy resources (DERs) [4]. In this regard, the development of interconnected multi-energy systems (MESs) can be contemplated as an appropriate and efficient solution which locally satisfies the end users' demands by utilizing renewable energy systems and multi-energy carriers in an integrated structure [5]. Indeed, MESs are the main building blocks of the future smart cities infrastructures. Therefore future smart cities have more sustainable and more efficient structure incorporating transactive features of interconnected MESs. To competent implementation of interconnected MESs, digitalized and advanced technologies should be regarded as a systematic communication infrastructure. The integration of new embedded computing, information technology, and control technologies are known as the Internet of Things (IoT). Studies show that IoT is a constructive platform improving interoperability of interconnected MESs [6]. Therefore assessment of the role of IoT in the interconnected MESs is considered as a significant subject investigating in the current chapter. An interconnected MES based on the IoT technology offers an operative framework for local energy trading among end users that is well known in the literature as peer-to-peer (P2P) energy trading. The application of P2P energy trading based on the advanced technologies such as IoT is addressed in literature. In Ref. [7], the IoT and blockchain technologies are used to present an efficient P2P energy trading pilot platform. In Ref. [8], the blockchain-enabled P2P energy society with multi-scale flexibility services is proposed in an energy community environment. In Ref. [9], the real-time virtual energy prosumer business model is proposed based on IoT technology. On the other hand, MESs provide vital interrelationships between energy, environment, and productivity which can improve all technical, social, and environmental sustainability [10]. The impacts of MESs' implementation on emission reduction and operation costs reduction are addressed in Refs. [11,12], while positive effects of MESs on reliability and flexibility are ensured in Ref. [12]. It is shown in Ref. [13] that MESs have a critical effect on system reliability. A flexible-reliable operation optimization model of interconnected MESs incorporating distributed generations, energy storage systems, and demand response is analyzed in Ref. [14].

In this regard, the main objectives of this chapter are as follows:

1. An overview of the integrated transactive structure and control methods of interconnected MESs is carried out.
2. The role of IoT technology in the interconnected MESs as a transactive energy (TE) structure is investigated.
3. Different types of uncertainty modeling approaches in the interconnected MESs are debated.
4. The benefits and challenges of interconnected MESs from different point of views such as technical, economic, environmental, and social are discussed.

This book chapter is established as follows: Section 2.2 gives the structure of independent and interconnected energy networks. Section 2.3 discusses about the importance of IoT framework in TE structure. Section 2.4 analyzes the control methods of MESs. Section 2.5 illustrates various modeling approaches in two parts: deterministic and nondeterministic modes, in which different uncertainty modeling methods are precisely demonstrated. In Section 2.6, benefits and challenges of MESs are discussed, while concluding remarks are summarized in Section 2.7.

2.2 Modern interconnected energy networks

Human society is currently seeking better solutions to integrate energy system structures, from demand side to supply side, in order to achieve more efficient and reliable energy system known as an MES. The MES can be defined as an optimal interaction among heat, electricity, fuels, cooling, and other energy components as well as energy carriers to improve economic, environmental, and technical performances compared to conventional energy systems [15]. Furthermore, a number of small-scale MESs can be interconnectedly operated in an integrated transactive structure. In the following subsections, the structure of independent and interconnected MES is more elucidated in details.

2.2.1 Independent multi-energy system

An MES is a small piece of a smart city puzzle in which various energy carriers such as electrical, thermal, gas, and water are employed. Under such an environment, an optimal coordination among energy conversion, storage, and generation units should be performed to determine the finest operating point of MES. Thus the required information of system operator, such as different energy carriers' prices, demands, characteristics of generation resources, conversion systems, and storage systems, should be provided by an IoT infrastructure. Now, the system operator optimizes the performance of MES by concentrating on preplanned targets. Accordingly, the operation commands are sent to all players including generation pattern, charging and discharging status, energy conversion commitment, and demand response implementation. The demand historical data can be also used to organize the energy efficiency programs as a midterm demand-side management

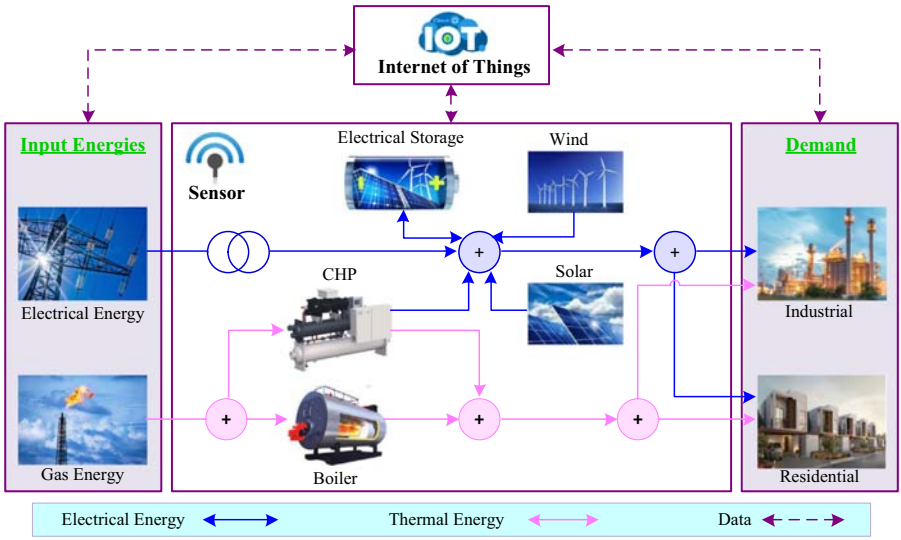


Figure 2.1 A schematic of a sample smart MES. *MES*, Multi-energy system.

program. A simple architecture of a smart MES is displayed in Fig. 2.1, whereas electrical and gas energy carries are contemplated as primal energy resources. However, other energy carriers such as cooling, thermal, and water can be also taken into consideration in the MES system. Referring to Fig. 2.1, it can be seen that a battery is merely considered as an electrical storage system, while other storage units like compressed-air energy storage (CAES) and power to gas (P2G) are also examined in some recent researches [16]. Furthermore, different renewable resources have been recently contemplated in the MES structure.

2.2.2 Interconnected multi-energy systems

Under a smart environment incorporating IoT, a number of MESs are interconnected where a TE structure may lead to new challenges in energy policy making, ranging from long-term to short-term strategies. Therefore, in an interconnected MES, the energy and data will be exchanged amongst MESs through an IoT system, whereas different types of excess energy can be shared to operate efficiently. In other words, under such a condition, every single MES can efficiently satisfy both demand and losses in adjacent MESs. Accordingly, in order to establish a decisive management, a system controller is desired to coordinate the operation of all independent MESs. Moreover, by strategically reacting to dispatching signals, the system coordinator acts as an interface between independent MESs and the power grid. Additionally, some important concerns such as particular mess, information privacy, and operation control may be resolved under interconnected MES [15]. Fig. 2.2 shows the structure of a simple smart interconnected MES.

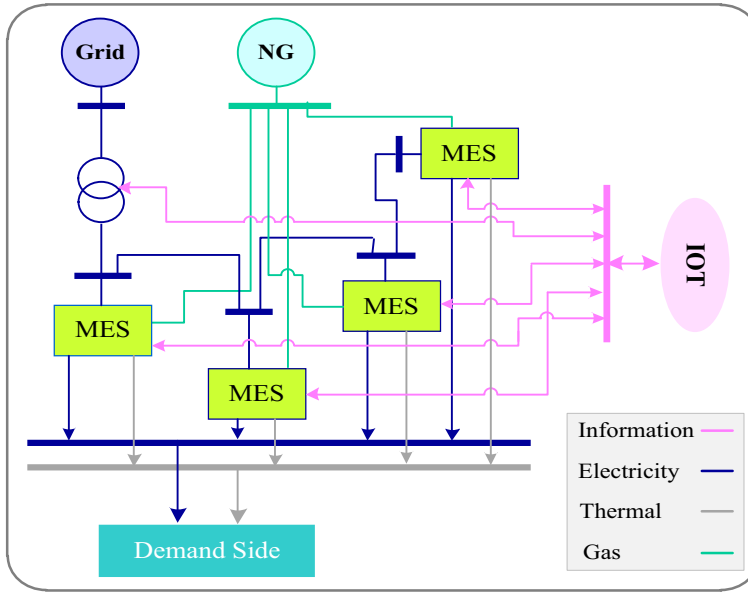


Figure 2.2 Architecture of a simple interconnected MES. *MES*, Multi-energy system.

2.3 Internet of Things technologies for transactive energy systems

The energy transition from a conventional energy system into a future democratic energy system brings several major challenges to energy research era [17]. The widespread use of DERs as well as adoption of demand-side management resources including demand response programs (DRPs) and energy efficiency programs can be considered as pivotal issues which show the necessity of integrated control in TE systems [18]. Utilizing an integrated control framework, both demand-side and supply-side resources can be simultaneously managed which is challenging due to a large number of smart elements in TE systems. However, the integrated control improves affordability, reliability, and sustainability of the future energy system which positively affects interoperability in energy systems [19]. In this regard, the GridWise Architecture Council (GWAC) held a seminar concentrating on novel ideas about the integrated control in 2011 [20]. The main achievement of this seminar was TE concept as a market-type solution. Referring to GWAC, TE is "*a set of economic and control mechanisms that allows the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter*." This definition emphasizes the active role of end users in a TE structure to manage the dynamic equilibrium of energy supply and demand. Accordingly, a modern smart ecosystem has been

efficiently established to integrate supplier−buyer relationship. In fact, TE market organizes intelligent devices to integrate automation systems and DERs concentrating on interoperability properties among all market participants [21]. To realize this concept, simultaneous development in an economic sector and control systems is required. Moreover, it should be mentioned that some beneficial attributes of TE systems such as interoperability, transaction, temporal variability, alignment of objectives, stability, and reliability have been affirmed in previous researches.

To competent implementation of TE structure, a smart and efficient infrastructure is desired to process the real-time data. Here, the IoT framework plays an important role to provide a systematic communication environment among TE market players which handle energy system problems. Today, rapid innovation flow in digital technologies can facilitate the development of TE structure which leads to a better management of grid activities via providing customer-friendly information. Referring to International Energy Agency (IEA), use of smart meters, intelligent sensors, IoT devices, and thermostats have been annually increased by around 20%, whereas a drastic growth has been planned in over the next few decades [22]. In the following, fundamental components of IoT-based TE systems are listed.

- *Sensors*: These components are electronic devices which can generate digital, optical, electrical, or data from a physical situation or an event. Sensors' output signals are processed by smart devices, and proper command will be sent. Here, the most crucial challenges are power rating, intelligence of level sensing, security, size, price, and interoperability.
- *Networks*: A reliable network path is needed to transmit collected signals from sensors. The network path can be employed wired or wireless technologies such as Wi-Fi, Bluetooth, cellular networks, Wi-Max, and Li-Fi. Here, security, latency, and power consumption can be contemplated as the most challenges of IoT-based systems' networks.
- *Cloud*: To perform actual data processing, a temporary or permanent space is required to keep the massive data which are transferred by network paths. An IoT cloud is a massive database network which can support a large number of devices in high-speed data storage, traffic management, and precise computational analysis. However, the IoT cloud is faced with different challenges such as cloud distribution in the network, data security, real-time accessibility, and storage capacity.
- *Analytics*: Here, comprehensive insights are provided to exactly analyze massive data which helps the users to detect anomalies in collected data and rapidly respond to prevent unintended situations. The key concerns of analytics component are information sorting from collected data, precision, and exactness.
- *Standards*: All activities in IoT networks, including network protocols such as Li-Fi, communication protocols such as HTTP, and data aggregation such as transformation, should be followed prespecified rules and regulation to communicate efficiently. Privacy and security provision, as well as unstructured data management standards, are critical challenges of IoT systems from standards aspect.
- *User Interface*: This part facilitates communication of users and devices. The design of interface should be user friendly, interactive, and low power consumption which can be considered as main challenges of design selection.

2.4 Control methods of interconnected energy networks

Today, using the MES concept, diverse types of energy infrastructure in different consumption sectors including agricultural, industrial, commercial, and residential can be efficiently connected which may improve the social welfare and system reliability and reduce different types of system risks. Under such a transactive structure, an appropriate platform for energy and data exchange between two different MESs is provided that is managed via an efficient control method depending on the level of energy consumption as well as MESs' scale. Hence, three control approaches, including *centralized*, *decentralized*, and *distributed*, are suggested to handle the interconnected MESs which are elaborated in the following subsections. Fig. 2.3 exhibits the control architecture of such interconnected MESs, while a concise comparison between these methods is presented in Table 2.1.

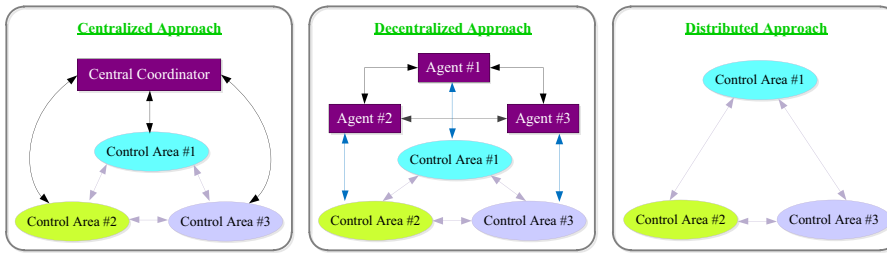


Figure 2.3 Drawing of control models of a simple interconnected energy system.

Table 2.1 Comparison between control methods of multi-energy system (MES).

	Centralized control	**Decentralized control**	**Distributed control**
Control	All regions are supervised by the central coordinator	Only one operator is responsible for each region	No central operator supervisory
Organization	Regions send data to a central coordinator	Data is exchanged between agents	Autonomous controllers are there in the entire system
Computational load	More than other methods	Lower than centralized control	Lower than centralized control
Fault	Influences the entire system	Only faulty region is not checked anymore, other zones are still under controlled	Does not influence the entire system
Profit	More than other methods	Lower than centralized control	Lower than centralized control

2.4.1 Centralized approach

Here, a central supervisory controller collects the information of MESs to solve the centralized optimization problem [23]. The main challenge of this approach is the reliability issue since a failure in the central controller affects the reliability of the entire system. Additionally, the point-to-point connections between MESs and central coordinator lead to a high computational process which complicates finding of an optimal operational decision [24]. Hence, this method merely works competently for small-scale systems. However, the computational complicacy and data processing might also be affected by the number of parameters and information.

The management of interconnected MESs is commonly performed by such centralized approach. As an example, the centralized control approach is used to handle the interconnected MESs incorporating DR and storage units in Ref. [25], while an optimal operation of centralized electrolysis-based hydrogen generation and storage systems is achieved in Ref. [26].

2.4.2 Decentralized approach

In a decentralized approach, each one of regions is handled by the self-control authority to provide a higher degree of reliability, while control decisions and information are shared between other regions. Here, the operator of an MES concentrates on its own profit maximization which is broken into several subproblems [27]. As provided in Table 2.1, the convergence time of this method is less in comparison with centralized approach. This issue occurs since the optimization process of different MESs can be parallelly performed, although MESs are connected. This privilege becomes more important when an area with multiple interconnected MES gets larger in size [23]. A novel voltage decentralized autonomous control strategy has been provided in Ref. [28] which is based on a multiagent system. A decentralized self-optimizing control method for residential multisplit air-conditioning systems is suggested in Ref. [29].

2.4.3 Distributed approach

Distributed control strategy as an effective control method that has been extensively examined in different field of domains including traffic control and process control [30]. This control strategy can also be employed to effectively manage interconnected MESs. In a distributed approach, each one of MESs accomplishes its self-optimization and individually schedules its components [31]. Here, the convergence time of optimal solution is more affected by size of interconnected MESs in comparison with previous approaches since a central supervisory controller is not accessible in distributed approach. Accordingly, information privacy and reliability level of interconnected MESs in this strategy can be more superior due to the lack of central coordinator. Although this approach is used to model energy systems, some researches declare that provided solution by distributed control strategies may not lead to a dominant global optimal solution [32]. The operation of a modular

photovoltaic (PV) generation system is optimized in Ref. [33] by using such distributed control strategy based upon improved DC bus signaling.

2.5 Modeling methods of interconnected multi-energy systems: a survey on state-of-the-art

The concept of an interconnected MES is formed by integrating small-scale MESs in a smart city. As mentioned before, the interconnected MES can drastically improve the system flexibility due to accessing various infrastructure such as resources, conversion units, and storage systems. However, the MES scheduling is an extremely complicated problem while considering uncertainties makes it even more sophisticated. Hence, different deterministic and nondeterministic modeling frameworks have been recently examined to overcome such complications which are reviewed in the following sections.

2.5.1 Deterministic approach

The deterministic modeling of an interconnected MES is typically performed based on the cost and benefit analysis arising, whereas the selection of time resolution in an optimization process is usually dependent on the upstream energy market price. However, the scheduling time horizon of an MES optimization problem can be altered from 24 hours to 1 year. As an example, an hourly scheduling of MES is addressed in Ref. [34] to minimize the operation costs over a 1-day horizon, whereas all parameters including energy price, demand, and power generation of distributed units are modeled by deterministic approaches. A deterministic model incorporating electrical vehicles is proposed in Ref. [35] while concentrating on minimization of operation expenditure and emitted pollutants over a 1-year horizon. Furthermore, from mathematical modeling point of view, deterministic models of MES can be structured as both mixed integer nonlinear programming problem and mixed integer linear programming problem [36], while various optimization methods such as classical [37], heuristic [38], and metaheuristic [39] approaches can be used to solve the interconnected MES optimization problem.

2.5.2 Nondeterministic approach

The application of renewable energies in an interconnected MES is one of the main reasons considering uncertainties in modeling process. Prices of energy carriers are also regarded as uncertain parameter depending on different factors such as sudden fluctuations in demand, unexpected outages of generation and infrastructure, as well as weather forecasting. Furthermore, the energy consumption in different sectors such as electrical, thermal, gas, and water cannot be precisely predictable. All these uncertainties of the interconnected MES can be modeled by various approaches which are comprehensively explained in next subsections.

2.5.2.1 Scenarios-based approach

The scenario-based method is a very prevalent approach to model the uncertainty which is used in cases that the historical data of uncertain events is accessible. The scenario-based uncertainty modeling approach has several stages as follows:

1. *Historical data gathering:* Here, the historical data of the uncertain event is collected, and the faulty data are refined.
2. *Fitting the probability distribution function (PDF) to historical data:* In this stage, the appropriate PDF should be selected as it is fitted into the historical data. Referring to previous studies in scenario-based uncertainty modeling issues, the normal PDF is a good candidate for modeling the uncertainty of demand and energy prices. Furthermore, Weibull and Beta PDFs are respectively used to model the power generation of wind and PV.
3. *Scenario generation:* The selected PDF in previous stage is a continuous function, thus the Monte Carlo approach is used to generate a sufficient number of scenarios. Therefore the continuous function is discretized without any violation of the problem generality.
4. *Scenario reduction:* Utilizing Monte Carlo approach, a large number of scenarios are generated which should be decreased via scenario reduction approaches. In this regard, the K-means and SCENRED functions in the GAMS environment can be used as popular scenario reduction tools.
5. *Applying selected scenarios to the MES model.*

In some researches associated with the MES scheduling, uncertainties of wind and PV generation as well as demand are modeled by the scenario-based approach. In Ref. [36], the scenario-based approach is used to model the nonshiftable demand and generation of PV system, while the Monte Carlo approach incorporating k-means is implemented to generate a sufficient number of scenarios. However, the backward scenario reduction technique is applied in Ref. [40]. In Ref. [41], the electrical vehicle uncertainty is modeled via a scenario-based approach and a special algorithm based on grasshopper search, while the future uncertainty in electricity price of MES is also dealt with grasshopper search.

2.5.2.2 Robust optimization

The robust optimization approach is one of the most appropriate methods for modeling uncertainties [42]. This method solves the problem under the worst-case scenario which guarantees the robustness of solution as a highly conservative resolution [43]. The objective function of the robust optimization is an NP-hard function with three sections. Some mathematical approaches such as Benders decomposition and column-and-constraint generation are used to relax the NP-hard robust optimization problem into a typical problem.

The robust optimization method is addressed in some researches to handle the energy management problem in MES. The planning and operation scheduling of the MES are simultaneously optimized by an adaptive robust optimization method in Ref. [44], where the objective function involves the minimization of investment cost in the first stage, worst scenario identification in the second stage, and minimization of operating cost in the third stage under the worst-case scenario. In Ref.

[45], the coordinated operation of interconnected MES is modeled by the robust optimization method.

2.5.2.3 Information gap decision theory

Information gap decision theory (IGDT) is a nonprobabilistic decision theory which is used when the historical data of the uncertain parameter is not accessible. Under the uncertain environment, this method seeks to maximize the robustness of the problem to failure or opportunity for windfall success [46]. Accordingly, two contrasting consequences of uncertainty are simultaneously raised [47]. Moreover, this approach facilitates the optimization process by conducting solving methods against the various uncertainties in a straightforward approach without necessitating PDF or membership function of corresponding uncertain variables [48].

The IGDT approach is recently addressed in MES optimization model. The IGDT-based robust scheduling of combined cooling, heat, and power is proposed in Ref. [49] to model the electrical price uncertainty. Uncertainties of renewable generation as well as electrical demand under extreme operational uncertainties are modeled by the IGDT approach in smart distribution network [50]. The hybrid stochastic/IGDT optimization method for the optimal scheduling of wind integrated MES is presented in Ref. [51], considering the uncertainties of wind power generation, energy price, and demands. The penetration rate of DRPs in MES scheduling has been modeled by the IGDT in Ref. [52].

2.5.2.4 Chance constraints

The chance-constrained uncertainty modeling method as a nonprobabilistic approach is used to solve optimization problems under various uncertainties. Here, the optimization problem is modeled so that ensuring probability of meeting a certain constraint is above a certain level. In fact, the chance constraints approach restricts the feasible region so that the solution confidence level becomes high. The chance-constrained method is relatively considered as a robust approach which is often difficult to solve.

The chance-constrained method is lately utilized in MES researches. In Ref. [53], a chance-constrained uncertainty modeling of planning and operation scheduling of an interconnected MES is addressed, while the suggested structure decreases operating expense and increases the penetration rate of renewable resources in planning horizon. The electrical and gas flow in an interconnected MES is modeled by the chance constraints approach in Ref. [54].

2.5.2.5 Fuzzy method

The fuzzy programming method is a useful and powerful tool when adequate input data for the uncertainty modeling is not available.

In Ref. [55], the fuzzy-based optimal scheduling of the MES is handled where the uncertainties of wind power generation, electrical load, and electricity price are

evaluated. In Ref. [56], utilizing fuzzy approach, the optimal location of renewable resources in Vietnam in the presence of uncertainties is nominated.

2.5.2.6 Z-number

The z-number uncertainty modeling approach was proposed in 2011 [57]. This method is the more comprehensive version of the fuzzy approach which models the uncertain parameter by two independent parts: *Probability* and *Possibility*. The PDF is used to model the probability part and the possibility part is determined by experts.

In previous studies of energy system, the z-number uncertainty modeling approach is commonly used to accurately model the uncertain parameters. In Ref. [58], the flexibility of smart power system considering DRPs is assessed, whereas the penetration rate of DRPs is modeled by z-number method. Moreover, a price elasticity−based model of DRPs is structured by z-number uncertainty modeling approach in Ref. [59].

2.5.2.7 Interval analysis

In some real-world problems, the uncertain input parameters are provided in terms of ranges or intervals. The interval analysis is applied to such systems, the parameters of which are described as intervals or ranges.

In an MES, some uncertain parameters are placed in certain range which can be modeled by interval analysis approach. The uncertainty of the PV generation in Ref. [60] and the uncertainty correlation between renewable resources (wind turbine and PV generation) as well as uncertainty of demand response in Refs. [61,62] have been modeled by the interval modeling approach. The operation of MES is handled by a hybrid stochastic-interval optimization approach in Ref. [63], while the energy price and other input uncertain parameters are modeled by interval uncertainty modeling approach.

2.6 Advantages and challenges of interconnected multi-energy systems

Investigation and concentration on different positive and negative aspects of implementing interconnected MES can be considered as crucial issues which provide the more secure and the more promising environment. In the following sections, the most important benefits and difficulties of using interconnected MES will be scrutinized.

2.6.1 Advantages

The interconnected MES structure can bring some benefits to system players, including improvement of economic efficiency, system resiliency, reliability, and

flexibility, as well as emission mitigation, which are elucidated in details in the following subsections.

2.6.1.1 Economic efficiency

Economic efficiency is the most significant benefit of networked MESs. It is clear that electrical energy demand shows cyclical fluctuations in a specified time horizon which is not coordinated with consumption pattern of other types of energy carriers. Accordingly, economic efficiency in MES can be achieved by using this potential and converting from one form of energy to another based on the conservation law constraint.

The improvement of economic efficiency has been verified in an integrated electrical and gas structure [64]. Moreover, in Ref. [65], it is shown that considering different alternative energy resources and conversion units has been led to economic efficiency enhancement during peak hours of electricity demand. It is worth mentioning that from target standpoint, the economic benefit (or cost) of MESs is contemplated in the objective function; however, some studies added the capital recovery rate to objective function to examine the life span of the MESs [66,67].

2.6.1.2 Emission abatement

In the last decade, the world environmental crisis is one of crucial concerns which motivates energy research institutes to find effective solutions to relieve emitted pollutants. The energy sector is a major contributor to greenhouse gas emissions and other types of air pollution that negatively affect the environment and human health. To overcome this environmental challenges, green energy resources become promising solutions [68]. Thus the development of small-scale green energy resources should be considered as a pivotal energy policy. Referring to IEA survey, renewable resources capacity has been drastically increased in recent years which denotes the importance of environmental issues [69].

The MES incorporating advanced control system can be regarded as the best structure to integrate small-scale green energy resources. It is affirmed that the environmental index of an MES is significantly declined in the presence of renewable energy resources [70]. Additionally, energy conversion units and storage systems such as combined heat and power (CHP), CAES, and P2G can efficiently amended the environmental impacts in energy system. As an example, the simulated results in Ref. [71] show that carbon dioxide emissions in MES have been reduced by 9.89% in the presence of P2G unit, since it is consuming the emitted carbon dioxide of CHP as well as boiler. Furthermore, in some researches related to MES scheduling, the emission abatement target is considered as part of the objective function along with the economic target, whereas the selection of MES operation point can be a considerable challenge for system operator. Supporting this issue, using the suggested multi-objective framework in Ref. [72], the 9.51% reduction in emitted pollutants has led to 5% increasing in operation cost.

2.6.1.3 Resiliency improvement

From the standpoint of end users, the resiliency issue of energy systems is one of the most crucial problems, where various natural disasters, such as floods and earthquakes, can violate the resiliency of traditional energy systems. In recent researches, the fast restoration time and the electrification of energy system are considered as the most important indices to assess resiliency. However, the presence of DRPs, electrical vehicles, energy storages, conversion units, and DERs can positively affect the resilience level of energy systems. Consequently, the MES can provide an appropriate infrastructure for implementation of such technologies. As an example, the impacts of electrical energy storage systems and DRPs on the resilience level of MES are appraised in Ref. [3].

2.6.1.4 Reliability enhancement

In an energy system, reliability concept refers to a system's ability to procure sufficient power in the quantity and quality demanded under safe operating conditions as well as short-term utility failures or spontaneous demand variations [73]. In interconnected MESs, energy demand (such as electrical, thermal, gas, and water) can be satisfied in various ways due to the availability of different types of resources, as well as storage and conversion systems. Hence, the supply of demand in MESs has more degrees of freedom in comparison with conventional systems. Furthermore, reliability indices such as expected energy not served, loss of load expectation, and loss of load probability will be improved due to the presence of DRPs, DERs, storage, and conversion units [14]. Components' maintenance and inspection in interconnected MESs can be performed such that the system reliability is higher than the conventional systems. Finally, it can be concluded that interconnected MESs can be considered as a useful and efficient structure from a reliability point of view.

2.6.1.5 Flexibility improvement

The energy system flexibility refers to "ability of a power system to reliably and cost-effectively manage the variability and uncertainty of demand and supply across all relevant timescales" [2]. The fast ramp resources such as micro turbines, energy storage technologies (such as batteries and CAES), and DRPs are the main sources of flexibility in energy systems [74]. Moreover, the use of a fast real-time local energy management system can improve the system flexibility. The interconnected MESs can provide an appropriate and efficient environment for implementation of such technologies which leads to higher flexibility compared with conventional system.

2.6.2 Challenges

Besides mentioned advantages, the interconnected MESs will be faced to different challenges as demonstrated in the following sections.

2.6.2.1 Economic risk

Today, the operational risk of interconnected MESs is increased by developing renewable energy policies. The system operator should select risk-averse/taker operation strategies which depends on its behavioral characteristics. Thus multifarious methods have been recently proposed to model the operational risk of interconnected MESs. The conditional value at risk and the downside risk approaches are commonly used to overcome such challenges.

2.6.2.2 Social challenges

Today, humanity faces a modern energy structure with completely different rules compared with conventional energy systems due to increasing penetration of interconnected MESs in World. As an example, P2P energy trading can be hosted by the novel interconnected MESs, whereas human is the main decision-maker of P2P energy trading. On such energy trading platform, the energy price has a dynamic feature, since the energy can be exchanged between end users who participate in a local energy market. Hence, risk-averse end users may prefer to avoid participation in the local energy market. Moreover, home energy management systems, which support network regulatory via demand monitoring, should also coordinate and manage the P2P trading in such a way that both system efficiency and human benefits become maximized. All these concerns and complexities can violate the social acceptance of modern energy structures such as interconnected MESs.

2.6.2.3 Technological challenges

The IoT, as a technological advancement pillar, plays a key role in the modern interconnected MESs. The concept of IoT refers to connecting *human* world and *things* in an appropriate way. Under the smart energy environment, IoT is capable of filling the gap between the real world and the virtual world by developing smart objects into energy systems. Thus, in an integrated energy system, each object is live and smart which can sense the surroundings environment, deliver data, and communicate with other ones. The functional blocks of IoT are identification, communication, sensing, computation, semantics, and services which can make the whole energy system smarter and more convenient. However, the IoT implementation in an interconnected MESs can bring some challenges which are addressed as follows:

- *Cybersecurity:* The cybersecurity of energy participants in interconnected MESs is considered as a vital challenge due to more possibilities of cyberattacks in different information layers. Thus the advanced security protection applications have focused on securing the network and cloud sections.
- *Connectivity:* This concept addresses the ability of devices, infrastructure, cloud, and applications to enable seamless information flow. Regarding the complexity feature of the IoT infrastructures, good connectivity can be an important challenge for planners in IoT-based energy systems.

- *Continuity:* The continuity operation of the IoT-based interconnected MESs is an important issue. Therefore concentrating on batteries lifetime and other consumable parts can be considered as an indispensible point to ensure the service continuity in IoT-based structure. As an example, in industrial and large-scale IoT infrastructures, a battery life span ranging from 5 to 10 years is acceptable.
- *Compliance*: The compliance of clouds, applications, and other elements is an extremely pivotal issue due to a large number of components in an interconnected IoT-based MESs. Thus various standards and instruments have been published by institutes to address the compliance challenge.
- Coexistence: Coexistence is about the ability of wireless device to reliably operate in the presence of other interfering signals. Nevertheless, diverse types of wireless devices from different brands may lead to difficulties in the coexistence of components in IoT-based MES infrastructures.

2.7 Conclusion

This chapter concentrates on introducing the energy system modernization by developing interconnected MESs which is already compatible with TE structure concept. Under such transactive structure, the optimal operation solution of interconnected MESs is determined so that different types of energy as well as data can be efficiently exchanged between all MES operators. This information exchange can be managed by various control structures clustering into (1) centralized, (2) decentralized, and (3) distributed approaches. Accordingly, to competent handling of interconnected MESs, the presence of advanced IoT-based systems is imperative. Moreover, interconnected MESs scheduling is an extremely complicated problem, and considering uncertain parameters such as uncertainties of renewable resources, unanticipated variations of energy carriers' price, and spontaneous fluctuations in demand makes it even more complex. To overcome these difficulties, various uncertainty modeling approaches such as Monte Carlo, robust optimization, IGDT, chance constraints, fuzzy methods, z-number, and interval analysis can be investigated. Moreover, the interconnected MESs will be faced to different concerns such as economic risk and social and technological challenges. Besides these challenges, the positive and efficient aspects of the interconnected MESs, such as improvement of economic efficiency, system resiliency, reliability, and flexibility, as well as emission mitigation, should be considered as crucial issues.

The main achievements of this chapter can be listed as follows:

- The MES as a TE structure supports various energy-related programs to improve flexibility, resiliency, and energy sustainability. Definitely, the future smart cities will be interconnected multi-energy systems.
- The IoT framework plays an important role to provide an appropriate communication between MESs. In fact, the IoT infrastructure positively affects the interoperability of interconnected MESs.
- Basic components of IoT-based system such as sensors, networks, cloud, analytics, standards, and user interface face to critical challenges in energy systems which should be taken into consideration in future researches.

- Widespread adoption of interconnected MESs requires the precise and comprehensive researches on challenges as well as advantages.
- Selection of an appropriate uncertainty modeling method has great significance in interconnected MES scheduling. As an example, it is shown that the scenario-based approaches are more applicable to model uncertainties of renewable generations.

References

[1] S. Suman, Hybrid nuclear-renewable energy systems: a review, J. Clean. Prod. 181 (2018) 166−177. Available from: https://doi.org/10.1016/j.jclepro.2018.01.262. Apr.
[2] J. Conti, P. Holtberg, J. Diefenderfer, A. LaRose, J.T. Turnure, L. Westfall, "International energy outlook 2016 with projections to 2040," 2016.
[3] J. Khayatzadeh, S. Soleymani, S.B. Mozafari, H.M. Shourkaei, Optimizing the operation of energy storage embedded energy hub concerning the resilience index of critical load, J. Energy Storage 48 (2022) 103999. Available from: https://doi.org/10.1016/j.est.2022.103999. Apr.
[4] G. Zhang, et al., A multi-agent deep reinforcement learning approach enabled distributed energy management schedule for the coordinate control of multi-energy hub with gas, electricity, and freshwater, Energy Convers. Manag. 255 (2022) 115340. Available from: https://doi.org/10.1016/j.enconman.2022.115340. Mar.
[5] M. Monemi Bidgoli, et al., Robust scheduling of hydrogen based smart micro energy hub with integrated demand response, Energy 20 (4) (2020) 114393. Available from: https://doi.org/10.1016/j.apenergy.2019.114195. Sep.
[6] K. Siozios, D. Anagnostos, D. Soudris, E. Kosmatopoulos, IoT for smart grids: design challenges and paradigms. 2019.
[7] M.J. A. Baig, M.T. Iqbal, M. Jamil, J. Khan, "IoT and blockchain based peer to peer energy trading pilot platform," in: 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Nov. 2020, pp. 0402−0406, https://doi.org/10.1109/IEMCON51383.2020.9284869.
[8] Y. Wu, Y. Wu, H. Cimen, J.C. Vasquez, J.M. Guerrero, P2P energy trading: blockchain-enabled P2P energy society with multi-scale flexibility services, Energy Rep. 8 (2022) 3614−3628. Available from: https://doi.org/10.1016/j.egyr.2022.02.074. Nov.
[9] S. Park, et al., Distributed energy IoT-based real-time virtual energy prosumer business model for distributed power resource, Sensors 21 (13) (2021) 4533. Available from: https://doi.org/10.3390/s21134533. Jul.
[10] M. Mostafavi Sani, A. Noorpoor, M. Shafie-Pour Motlagh, Optimal model development of energy hub to supply water, heating and electrical demands of a cement factory, Energy 177 (2019) 574−592. Available from: https://doi.org/10.1016/j.energy.2019.03.043. Jun.
[11] A.A. Eladl, M.I. El-Afifi, M.A. Saeed, M.M. El-Saadawi, Optimal operation of energy hubs integrated with renewable energy sources and storage devices considering CO2 emissions, Int. J. Electr. Power Energy Syst. 117 (2020) 105719. Available from: https://doi.org/10.1016/j.ijepes.2019.105719. May.
[12] A.A.M. Aljabery, H. Mehrjerdi, S. Mahdavi, R. Hemmati, Multi carrier energy systems and energy hubs: comprehensive review, survey and recommendations, Int. J. Hydrog.

Energy 46 (46) (2021) 23795−23814. Available from: https://doi.org/10.1016/J.IJHYDENE.2021.04.178. Jul.

[13] A. Malekijavan, M. Aslinezhad, H. Zaferani, Reliability-based operation in energy hubs with several energy networks, Int. J. Ind. Electron. Control. Optim. 4 (4) (2021) 433−444. Available from: https://doi.org/10.22111/ieco.2021.36021.1310.

[14] A. Dini, A. Hassankashi, S. Pirouzi, M. Lehtonen, B. Arandian, A.A. Baziar, A flexible-reliable operation optimization model of the networked energy hubs with distributed generations, energy storage systems and demand response, Energy 239 (2022) 121923. Available from: https://doi.org/10.1016/j.energy.2021.121923. Jan.

[15] Y. Cheng, P. Zhang, X. Liu, Collaborative autonomous optimization of interconnected multi-energy systems with two-stage transactive control framework, Energies 13 (1) (2019). Available from: https://doi.org/10.3390/en13010171.

[16] P. Aliasghari, M. Zamani-Gargari, B. Mohammadi-Ivatloo, Look-ahead risk-constrained scheduling of wind power integrated system with compressed air energy storage (CAES) plant, Energy 160 (2018) 668−677. Available from: https://doi.org/10.1016/J.ENERGY.2018.06.215. Oct.

[17] M. Daneshvar, M. Pesaran, B. Mohammadi-ivatloo, Transactive energy integration in future smart rural network electrification, J. Clean. Prod. 190 (2018) 645−654. Available from: https://doi.org/10.1016/J.JCLEPRO.2018.04.043. Jul.

[18] M. Daneshvar, B. Mohammadi-ivatloo, K. Zare, Integration of distributed energy resources under the transactive energy structure in the future smart distribution networks, Operation of Distributed Energy Resources in Smart Distribution Networks, Elsevier, 2018, pp. 349−379.

[19] M. Daneshvar, S. Asadi, CPS-based transactive energy technology for smart grids, Cyber-Physical Systems in the Built Environment, Springer International Publishing, Cham, 2020, pp. 323−338.

[20] D. Forfia, M. Knight, R. Melton, The view from the top of the mountain: building a community of practice with the GridWise transactive energy framework, IEEE Power Energy Mag. 14 (3) (2016) 25−33. Available from: https://doi.org/10.1109/MPE.2016.2524961. May.

[21] R. Ambrosio, Transactive energy systems [Viewpoint], IEEE Electrif. Mag. 4 (4) (2016) 4−7. Available from: https://doi.org/10.1109/MELE.2016.2614234. Dec.

[22] International Energy Agency (IEA), "Digitalization & Energy," 2017. https://doi.org/10.1787/9789264286276-en.

[23] M. Mohammadi, Y. Noorollahi, B. Mohammadi-ivatloo, M. Hosseinzadeh, H. Yousefi, S.T. Khorasani, Optimal management of energy hubs and smart energy hubs − a review, Renew. Sustain. Energy Rev. 89 (2018) 33−50. Available from: https://doi.org/10.1016/j.rser.2018.02.035. September 2017.

[24] T. Dragicevic, D. Wu, Q. Shafiee, L. Meng, Distributed and decentralized control architectures for converter-interfaced microgrids, Chin. J. Electr. Eng. 3 (2) (2017) 41−52. Available from: https://doi.org/10.23919/CJEE.2017.8048411.

[25] D. Huo, S. Le Blond, C. Gu, W. Wei, D. Yu, Optimal operation of interconnected energy hubs by using decomposed hybrid particle swarm and interior-point approach, Int. J. Electr. Power Energy Syst. 95 (2018) 36−46. Available from: https://doi.org/10.1016/j.ijepes.2017.08.004. Feb.

[26] H.E.Z. Farag, A. Al-Obaidi, H. Khani, N. El-Taweel, E.F. El-Saadany, H.H. Zeineldin, Optimal operation management of distributed and centralized electrolysis-based hydrogen generation and storage systems, Electr. Power Syst. Res. 187 (2020) 106476. Available from: https://doi.org/10.1016/j.epsr.2020.106476. Oct.

[27] L. Bakule, Decentralized control: an overview, Annu. Rev. Control. 32 (1) (2008) 87–98. Available from: https://doi.org/10.1016/j.arcontrol.2008.03.004.
[28] N. Yorino, Y. Zoka, M. Watanabe, "An optimal autonomous decentralized control method for voltage control devices by using a multi-agent system," pp. 1–9, 2014.
[29] Z.Y. Zhang, C.L. Zhang, F. Xiao, Energy-efficient decentralized control method with enhanced robustness for multi-evaporator air conditioning systems, Appl. Energy 279 (2020) 115732. Available from: https://doi.org/10.1016/J.APENERGY.2020.115732. Dec.
[30] W. Wang, Z. Lu, Cyber security in the smart grid: survey and challenges, Comput. Netw. 57 (5) (2013) 1344–1371. Available from: https://doi.org/10.1016/J.COMNET.2012.12.017. Apr.
[31] F. Khavari, A. Badri, A. Zangeneh, M. Shafiekhani, "A comparison of centralized and decentralized energy-management models of multi-microgrid systems," in: IEEE Proc. 2017 Smart Grid Conf. SGC 2017, vol. 2018-Janua, pp. 1–6, 2018, https://doi.org/10.1109/SGC.2017.8308837.
[32] K. Umer, Q. Huang, M. Khorasany, M. Afzal, W. Amin, A novel communication efficient peer-to-peer energy trading scheme for enhanced privacy in microgrids, Appl. Energy 296 (2021) 117075. Available from: https://doi.org/10.1016/j.apenergy.2021.117075. Aug.
[33] K. Sun, L. Zhang, Y. Xing, J.M. Guerrero, A distributed control strategy based on DC bus signaling for modular photovoltaic generation systems with battery energy storage, IEEE Trans. Power Electron. 26 (10) (2011) 3032–3045. Available from: https://doi.org/10.1109/TPEL.2011.2127488.
[34] A.R. Namjoo, R. Dashti, S. Dorahaki, H.R. Shaker, A novel enviro-economic three-stage market-based energy management considering energy storage systems and demand response programs for networked smart microgrids, Electr. Eng. (2022). Available from: https://doi.org/10.1007/s00202-022-01510-x. Mar.
[35] M. Mittelviefhaus, G. Georges, K. Boulouchos, Electrification of multi-energy hubs under limited electricity supply: De-/centralized investment and operation for cost-effective greenhouse gas mitigation, Adv. Appl. Energy 5 (2022) 100083. Available from: https://doi.org/10.1016/j.adapen.2022.100083. Feb.
[36] S. Dorahaki, M. Rashidinejad, S.F. Fatemi Ardestani, A. Abdollahi, M.R. Salehizadeh, A home energy management model considering energy storage and smart flexible appliances: A modified time-driven prospect theory approach, J. Energy Storage 48 (2022) 104049. Available from: https://doi.org/10.1016/j.est.2022.104049. Apr.
[37] S. Dorahaki, A. Abdollahi, M. Rashidinejad, M. Moghbeli, The role of energy storage and demand response as energy democracy policies in the energy productivity of hybrid hub system considering social inconvenience cost, J. Energy Storage (2020) 102022. Available from: https://doi.org/10.1016/j.est.2020.102022. Oct.
[38] M.S. Javadi, A. Esmaeel Nezhad, A.R. Jordehi, M. Gough, S.F. Santos, J.P.S. Catalão, Transactive energy framework in multi-carrier energy hubs: a fully decentralized model, Energy 238 (2022) 121717. Available from: https://doi.org/10.1016/j.energy.2021.121717. Jan.
[39] M. AkbaiZadeh, T. Niknam, A. Kavousi-Fard, Adaptive robust optimization for the energy management of the grid-connected energy hubs based on hybrid meta-heuristic algorithm, Energy 235 (2021) 121171. Available from: https://doi.org/10.1016/j.energy.2021.121171. Nov.
[40] S.A. Mansouri, A. Ahmarinejad, M.S. Javadi, J.P.S. Catalão, Two-stage stochastic framework for energy hubs planning considering demand response programs, Energy 206 (2020) 118124. Available from: https://doi.org/10.1016/j.energy.2020.118124. Sep.

[41] R. Li, S. SaeidNahaei, Optimal operation of energy hubs integrated with electric vehicles, load management, combined heat and power unit and renewable energy sources, J. Energy Storage 48 (2022) 103822. Available from: https://doi.org/10.1016/j.est.2021.103822. Apr.

[42] X. Zhu, B. Zeng, H. Dong, J. Liu, An interval-prediction based robust optimization approach for energy-hub operation scheduling considering flexible ramping products, Energy 194 (2020) 116821. Available from: https://doi.org/10.1016/j.energy.2019.116821. Mar.

[43] S.A. Mansouri, M.S. Javadi, A robust optimisation framework in composite generation and transmission expansion planning considering inherent uncertainties, J. Exp. Theor. Artif. Intell. 29 (4) (2017) 717−730. Available from: https://doi.org/10.1080/0952813X.2016.1259262. Jul.

[44] S. Karamdel, M.P. Moghaddam, Robust expansion co-planning of electricity and natural gas infrastructures for multi energy-hub systems with high penetration of renewable energy sources, IET Renew. Power Gener. 13 (13) (2019) 2287−2297. Available from: https://doi.org/10.1049/iet-rpg.2018.6005. Oct.

[45] X. Lu, Z. Liu, L. Ma, L. Wang, K. Zhou, S. Yang, A robust optimization approach for coordinated operation of multiple energy hubs, Energy 197 (2020) 117171. Available from: https://doi.org/10.1016/j.energy.2020.117171. Apr.

[46] F. Mumtaz, I.S. Bayram, Planning, Operation, and Protection of Microgrids: An Overview, Energy Procedia 107 (2017) 94−100. Available from: https://doi.org/10.1016/j.egypro.2016.12.137.

[47] M. Kafaei, D. Sedighizadeh, M. Sedighizadeh, A.S. Fini, An IGDT/Scenario based stochastic model for an energy hub considering hydrogen energy and electric vehicles: a case study of Qeshm Island, Iran, Int. J. Electr. Power Energy Syst. 135 (2022) 107477. Available from: https://doi.org/10.1016/j.ijepes.2021.107477. Feb.

[48] S.E. Ahmadi, N. Rezaei, An IGDT-based robust optimization model for optimal operational planning of cooperative microgrid clusters: a normal boundary intersection multi-objective approach, Int. J. Electr. Power Energy Syst. 127 (2021) 106634. Available from: https://doi.org/10.1016/j.ijepes.2020.106634. May.

[49] A.R. Jordehi, M.S. Javadi, M. Shafie-khah, J.P.S. Catalão, Information gap decision theory (IGDT)-based robust scheduling of combined cooling, heat and power energy hubs, Energy 231 (2021) 120918. Available from: https://doi.org/10.1016/j.energy.2021.120918. Sep.

[50] M. Khajehvand, A. Fakharian, M. Sedighizadeh, A risk-averse decision based on IGDT/stochastic approach for smart distribution network operation under extreme uncertainties, Appl. Soft Comput. 107 (2021) 107395. Available from: https://doi.org/10.1016/j.asoc.2021.107395. Aug.

[51] S. Pazouki, et al., Short-term scheduling strategy for wind-based energy hub: a hybrid stochastic/IGDT approach, Int. J. Electr. Power Energy Syst. 80 (1) (2019) 113825. Available from: https://doi.org/10.1016/j.ijepes.2016.01.044. Sep.

[52] M. Vahid-Ghavidel, J.P.S. Catalao, M. Shafie-khah, S.S. Barhagh, B. Mohammadi-Ivatloo, IGDT opportunity method in the trading framework of risk-seeker demand response aggregators, 2019 IEEE Milan. PowerTech (2019) 1−6. Available from: https://doi.org/10.1109/PTC.2019.8810601. Jun.

[53] D. Huo, C. Gu, D. Greenwood, Z. Wang, P. Zhao, J. Li, Chance-constrained optimization for integrated local energy systems operation considering correlated wind generation, Int. J. Electr. Power Energy Syst. 132 (2021) 107153. Available from: https://doi.org/10.1016/j.ijepes.2021.107153. Nov.

[54] D. Huo, C. Gu, K. Ma, W. Wei, Y. Xiang, S. Le Blond, Chance-constrained optimization for multienergy hub systems in a smart city, IEEE Trans. Ind. Electron. 66 (2) (2019) 1402−1412. Available from: https://doi.org/10.1109/TIE.2018.2863197. Feb.

[55] M. Mohammadi, Y. Noorollahi, B. Mohammadi-ivatloo, Fuzzy-based scheduling of wind integrated multi-energy systems under multiple uncertainties, Sustain. Energy Technol. Assess. 37 (2020) 100602. Available from: https://doi.org/10.1016/j.seta.2019.100602. Feb.

[56] C.-N. Wang, Y.-F. Huang, Y.-C. Chai, V. Nguyen, A multi-criteria decision making (MCDM) for renewable energy plants location selection in Vietnam under a fuzzy environment, Appl. Sci. 8 (11) (2018) 2069. Available from: https://doi.org/10.3390/app8112069. Oct.

[57] L.A. Zadeh, A note on Z-numbers, Inf. Sci. (Ny). 181 (14) (2011) 2923−2932. Available from: https://doi.org/10.1016/j.ins.2011.02.022. Jul.

[58] S. Poorvaezi-Roukerd, A. Abdollahi, W. Peng, Flexibility-constraint integrated resource planning framework considering demand and supply side uncertainties with high dimensional dependencies, Int. J. Electr. Power Energy Syst. 133 (2021) 107223. Available from: https://doi.org/10.1016/j.ijepes.2021.107223. Dec.

[59] B. Zeng, X. Zhu, C. Chen, Q. Hu, D. Zhao, J. Liu, Unified probabilistic energy flow analysis for electricity−gas coupled systems with integrated demand response, IET Gener. Transm. Distrib. 13 (13) (2019) 2697−2710. Available from: https://doi.org/10.1049/iet-gtd.2018.6877. Jul.

[60] M. Kaffash, G. Ceusters, G. Deconinck, Interval optimization to schedule a multi-energy system with data-driven PV uncertainty representation, Energies 14 (10) (2021) 2739. Available from: https://doi.org/10.3390/en14102739. May.

[61] W. Wang, et al., An interval optimization-based approach for electric−heat−gas coupled energy system planning considering the correlation between uncertainties, Energies 14 (9) (2021) 2457. Available from: https://doi.org/10.3390/en14092457. Apr.

[62] M. Barzegar, M. Rashidinejad, M. MollahassaniPour, A. Bakhshai, H. Farahmand, A techno-economic assessment of energy efficiency in energy management of a micro grid considering green-virtual resources, Sustain. Cities Soc. 61 (2020) 102169. Available from: https://doi.org/10.1016/J.SCS.2020.102169. Oct.

[63] M. Sharafi, T.Y. ElMekkawy, Stochastic optimization of hybrid renewable energy systems using sampling average method, Renew. Sustain. Energy Rev. 52 (2015) 1668−1679. Available from: https://doi.org/10.1016/J.RSER.2015.08.010. Dec.

[64] M. Gil, P. Duenas, J. Reneses, Electricity and natural gas interdependency: comparison of two methodologies for coupling large market models within the European Regulatory Framework, IEEE Trans. Power Syst. 31 (1) (2016) 361−369. Available from: https://doi.org/10.1109/TPWRS.2015.2395872. Jan.

[65] E.A. Martinez Cesena, E. Loukarakis, N. Good, P. Mancarella, Integrated electricity−heat−gas systems: techno−economic modeling, optimization, and application to multi-energy districts, Proc. IEEE 108 (9) (2020) 1392−1410. Available from: https://doi.org/10.1109/JPROC.2020.2989382. Sep.

[66] T. Adefarati, R.C. Bansal, Reliability and economic assessment of a microgrid power system with the integration of renewable energy resources, Appl. Energy 206 (2017) 911−933. Available from: https://doi.org/10.1016/j.apenergy.2017.08.228. Nov.

[67] A. Shahmohammadi, M. Moradi-Dalvand, H. Ghasemi, M.S. Ghazizadeh, Optimal design of multicarrier energy systems considering reliability constraints, IEEE Trans. Power Deliv. 30 (2) (2015) 878−886. Available from: https://doi.org/10.1109/TPWRD.2014.2365491. Apr.

[68] M.C. Lott, S. Pye, P.E. Dodds, Quantifying the co-impacts of energy sector decarbonisation on outdoor air pollution in the United Kingdom, Energy Policy 101 (2017) 42−51. Available from: https://doi.org/10.1016/j.enpol.2016.11.028. Feb.

[69] IEA, "Renewables 2021," International Energy Agency Publication., p. 167, 2021, [Online]. Available: http://www.iea.org/t&c/%0Ahttps://webstore.iea.org/download/direct/4329.

[70] S. Taqvi, A. Almansoori, A. Elkamel, Optimal renewable energy integration into the process industry using multi-energy hub approach with economic and environmental considerations: Refinery-wide case study, Comput. Chem. Eng. 151 (2021) 107345. Available from: https://doi.org/10.1016/j.compchemeng.2021.107345. Aug.

[71] S.A. Mansouri, E. Nematbakhsh, A. Ahmarinejad, A.R. Jordehi, M.S. Javadi, S.A.A. Matin, A Multi-objective dynamic framework for design of energy hub by considering energy storage system, power-to-gas technology and integrated demand response program, J. Energy Storage 50 (2022) 104206. Available from: https://doi.org/10.1016/j.est.2022.104206. Jun.

[72] M. Monemi Bidgoli, H. Karimi, S. Jadid, A. Anvari-Moghaddam, Stochastic electrical and thermal energy management of energy hubs integrated with demand response programs and renewable energy: A prioritized multi-objective framework, Electr. Power Syst. Res. 196 (2021) 107183. Available from: https://doi.org/10.1016/j.epsr.2021.107183. Jul.

[73] M. Nazari-heris, S. Asadi, B. Mohammadi-ivatloo, Planning and operation of multi-carrier energy networks, no. January. 2021.

[74] S. Dorahaki, R. Dashti, H.R. Shaker, Optimal outage management model considering emergency demand response programs for a smart distribution system, Appl. Sci. 10 (21) (2020) 7406. Available from: https://doi.org/10.3390/app10217406. Oct.

Overview of Internet of Things-based fault positioning cyber-physical systems in smart cleaner multi-energy systems

3

Mahdi Ghanbarzaad Khajeh, Hadi Vatankhah Ghadim and Jaber Fallah Ardashir
Department of Electrical Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran

Chapter Outline

3.1 Introduction

The Internet of Things (IoT) influences our lifestyle from a behavioral perspective. From controllable air conditioners to electrical vehicles or smartwatches which track daily activities, all of them are the general applications of IoT. They construct a network of interconnected devices with data flow between each other and the

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00005-7

control unit [1]. These data are usually obtained via sensors and are about their usage and the environment's condition. Sensors are usually available in any device that is within an IoT network, such as mobile phones, electrical appliances, and barcode sensors. These sensors gather and transmit data about the working state of the aforementioned devices. The data that is obtained from these sensors can be used to improve our lifestyle, and the efficiency of devices, and ease the user access to refined data about the usage pattern of each device. In summary, an IoT network is a communication platform for the connected devices to share the obtained data from their operating environment. The obtained data is sent to the computing center to analyze the necessary specifications and improve the application of the devices [2]. Finally, the interpreted information is shared with other devices to provide a better user experience, more automation in the processes, and improved efficiency in the performance of the devices in this network.

IoT is one of the gravitating developments nowadays. The idea of IoT was first presented by the Massachusetts Institute of Technology [3]. The idea of IoT was to connect different devices through a wireless communication channel to create a central control unit. The main intentions behind this technology were to ease the access of the user to the information about the owned assets while providing easy controllability. IoT has been adopted by many users for various purposes since then. The main application of IoT in modern power systems is the integration of power and communication networks and the usage of multiple sensors to optimize the operation of the grid, as seen in Fig. 3.1. The integration of IoT technology in modern power systems resulted in the creation of cyber-physical power systems (CPPSs). In short, CPPSs are power systems in which the network-based control assets are used to connect the physical infrastructure using wireless communication protocols to provide higher flexibility and accessibility for control parameters [4].

The implementation of IoT technology in the operation of power systems relies upon online monitoring and real-time control in all aspects of grid management, such as state estimation, unit commitment, and infrastructure protection. The primary characteristics of IoT-based power systems are grid information, communication, and automation. Meanwhile, IoT technology is used to implement [5,6]:

- the complete perception of the grid,
- reliable transmission of data, and
- intelligent analysis of the obtained data.

One of the most critical challenges in power systems is blackouts [7]. Approximately, 10% of the total generation capacity is lost during the power transmission process [8]. Fault occurrences and sequential contingency events in transmission and distribution systems will lead to power system blackouts, and it is challenging to locate the failure [9,10]. IoT technology used in overhead transmission lines assists operators with line state monitoring and performance improvement of power transmission lines in operation conditions simultaneously. Various operational states include but are not limited to different meteorological conditions, ground wire vibration, components temperature, voltage sag, and power line windage yaw [11,12].

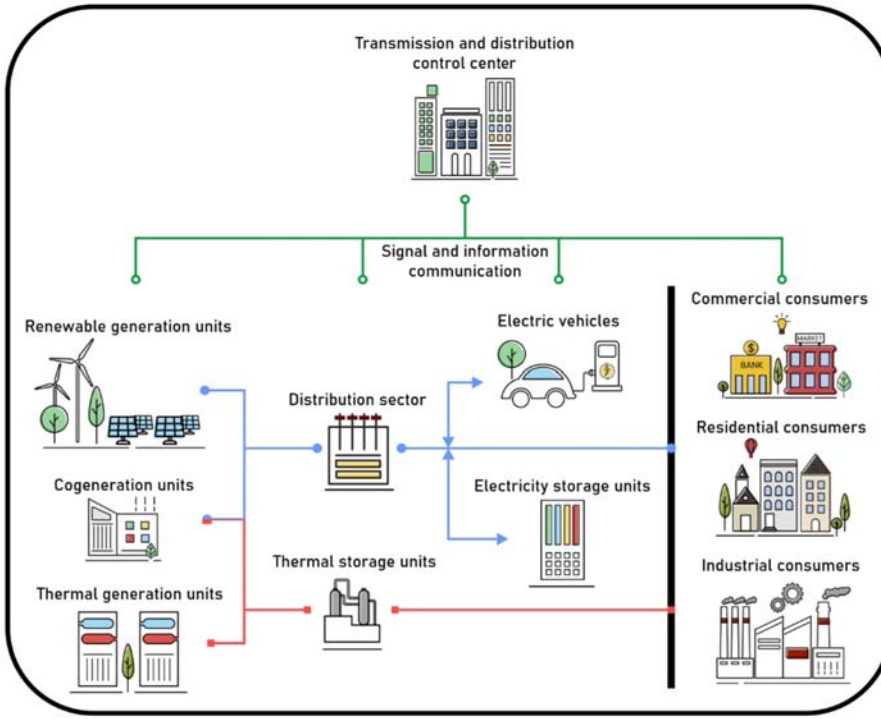


Figure 3.1 A schematic view of the integration of the electrical energy infrastructure with a communication network.

Integration of IoT and machine learning technologies will help the operators to overcome real-time difficulties. Grid operators will be able to integrate the communication and electrical power systems infrastructure effectively to increase the observability rate of the power system and improve the operational efficiency of the electrical infrastructure. If IoT technology is used in protection services of smart grids (SGs), such as real-time monitoring, maintenance, and fault location detection in the generation, transmission, and distribution section, the performance of the grid operators can be profoundly improved.

The rapid growth of electricity demand has become one of the complicated challenges in modern systems. To meet these changes in the state of the grid and to reduce the grid expansion costs, various network designs such as intelligent multicarrier energy grids are introduced [13]. The distribution of renewable power generation units and other clean energy generation sources in these energy systems will require the construction of additional transmission and distribution lines. Also, the establishment of energy storage systems and their application in providing necessary supply capacity, ancillary services [14], and optimizing renewable resource allocation in nonlinear demand profiles of consumption categories [15] will create multiple connection nodes in the power lines. Therefore it is predicted that future power systems will experience far more challenges in the fault monitoring issue.

They will be forced to function at their operating limits instead of generating power at total capacity. Dealing with increased usage of energy in times of failure is one of the vital concerns which needs extra attention. In terms of transmission lines, accurate fault positioning and classification are important since they transmit power over long distances [16]. Thus this will lead to a better understanding of the issue for the maintenance team. On the other hand, it will reduce the outage time. As a result, with the assistance of wide area monitoring control and protection, it is possible to reduce repair expenses and financial losses [17]. Also, consumer satisfaction could be heightened.

Distribution networks are one of the most essential segments of SGs. A wide range of decisions in the distribution network is made without adequate information technology and technical support. Safety technologies and management methods should be taken into account to achieve the power system reliability and power quality, as the complexity of distribution networks increases. Thus IoT can play a pivotal role in obtaining this goal by providing online state monitoring and accurate fault location after a system failure, thereby improving the efficiency and reliability of distribution networks [18].

Power grids have been facing challenges due to inappropriate and unreliable communication channels. Also, considering the high penetration rate of distributed generations (DGs) in modern power systems, real-time monitoring of transmission and distribution networks has encountered some disorders. IoT-based power system monitoring schemes can be a good solution to address these issues. A few reasons that motivate and encourage us to benefit from IoT in online monitoring and control of both transmission and distribution networks are listed below:

- IoT increases the efficiency of electricity transmission and distribution in the speed, reliability, and observability indexes.
- IoT avoids inaccurate operation of protective devices within DG-integrated grids.
- IoT reduces operational and maintenance costs of grid components.

In this chapter, studying the impact of IoT on online efficient monitoring of transmission and distribution lines is the main goal. Moreover, how IoT can improve the fault positioning of power networks, applications, challenges, and future opportunities will also be discussed.

3.2 Structure of Internet of Things-based fault monitoring cyber-physical system for clean multi-energy mixes

One of the most common applications of IoT in SGs is the Power Internet of Things (PIoT). Overhead transmission lines are vulnerable to different types of faults, which can be occurred due to extreme weather status, technical failures, and human errors similar to other sections of the grid. Some of these faults are illustrated in Fig. 3.2. Therefore it is essential to recognize the exact fault location.

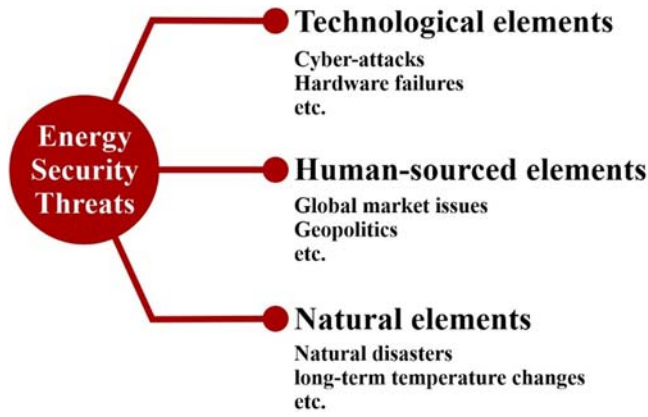


Figure 3.2 Categories of possible security threats in modern power systems.

Moreover, online monitoring of the transmission lines gives the opportunity of being aware of the system state at any moment. It is quite a challenging task for grid operators to look for the fault location in the transmission line physically. Furthermore, the whole network cannot be shut down to locate and clear the fault due to the financial losses and consumer dissatisfaction.

Transmission lines are more likely to be exposed to failures such as thundering, lightning phenomena, and short circuits. In IoT-based online monitoring of transmission lines, the entire power network grid has been divided into subsections, each of which will have small sections. There are some nodes between each substation and small stations composed of current and voltage sensors. These nodes are placed on every transmission line that supplies energy to industrial sectors or households. Using communication devices such as Wi-Fi modules, optical fiber, and microcontroller units, a connection link is provided between the nodes and substations. There should also be a cloud computing infrastructure to deliver and transport data and various files across the IoT data centers [19]. The received data by the nodes, including the state of power flow and the relays, can assist cloud computing to analyze and determine the section in a grid that needs to be isolated to prevent the expansion of the failure impact radius. The data are stored in the cloud for further analysis and real-time processes such as fault diagnosing throughout the line.

It is noteworthy that in the earlier versions of the IoT-based protection system, an alarm signal is issued to the operators to take the necessary preventive actions after analyzing the collected data. In that case, there is a strong possibility that the power grid will face severe damage due to the processing delay. To address this problem, the operating time should be reduced by adding a signal transmitter and a signal receiver to the old sensors to perceive the content of sending and receiving a detection signal before transmitting the data to the data center. As a result, operators locate the exact location of the short circuit based on the acquired data and take promising steps at an earlier stage before causing irreparable damage.

Eventually, the power distribution system delivers the electricity from the transmission network to the customers. Grid management becomes more challenging day by day with the expansion of the grid. Also, the power distribution grid is becoming progressively dynamic, increasing the complexity of the operation and the volume of data that the operator needs to analyze and operate the grid based on them. Fault location methods in distribution networks can be divided into the impedance and traveling wave method based on the Feeder Terminal Unit method and voltage sag information during the short circuit [20]. With the assistance of the IoT in the distribution network, all the industrial and residential power customers exchange data with each other, which paves the way for having a productive connection between the grid and the consumers. As a result, the grid network no longer uses one information source. Recently, the share of the inverter-interfaced distributed generators (IIDGs) such as photovoltaic or wind power stations has increased remarkably in the energy mix of the modern power systems due to their environmental and economic benefits. Therefore the role of the IIDGs on the distribution network fault flow should be taken into a significant source of concern.

When a fault occurs in the distribution network while a DG unit has connected to the grid, the short-circuit current tends to be a part of the fault current. Due to the existence of the DGs, the power flow is bidirectional. In distribution networks, distribution phasor measurement unit (D-PMU) is defined as one of the critical PIoT devices [18]. D-PMU can measure the voltage and current signals of the distribution networks under both stable and abnormal conditions. The D-PMU and GPS technologies measure the real-time three-phase fundamental voltage, current, angle, and other essential data. These measurement data and samples should be from a few cycles before and after the fault occurrence [21]. After the data sampling process, data is sent to an intelligent control center which is one of the main parts for dynamic monitoring, protection, and fault diagnosis. Amplitude and angle of three-phase voltage and current of fundamental positive sequence network are measured by D-PMU. This information is the main requirement for the fault location process. As various nodes are configured with different sensors in different places in the distribution network, D-PMU can be added to these nodes. In that case, the voltage and current of the nodes will be known, and fault location can be calculated using the obtained information [18].

Developed IoT-based power systems intend to utilize up-to-date technologies and various types of communication means to improve the human-to-thing and thing-to-thing real-time data exchange simultaneously. The objective of IoT-based power systems is to have a real-time and high-speed energy transmission and improve the intelligent functionality of power networks in case of any critical decision-making. With the assistance of Information and Communications Technology (ICT), a considerable amount of data is collected and analyzed. The mentioned goals can be achieved far more swiftly than it was in the past. Also, comparing the modern and traditional power systems clarifies that the development of various technologies such as Artificial Intelligence, IoT and other advanced communication means enhanced the linkage of all parts of the power system to have a better state awareness of every asset in the system.

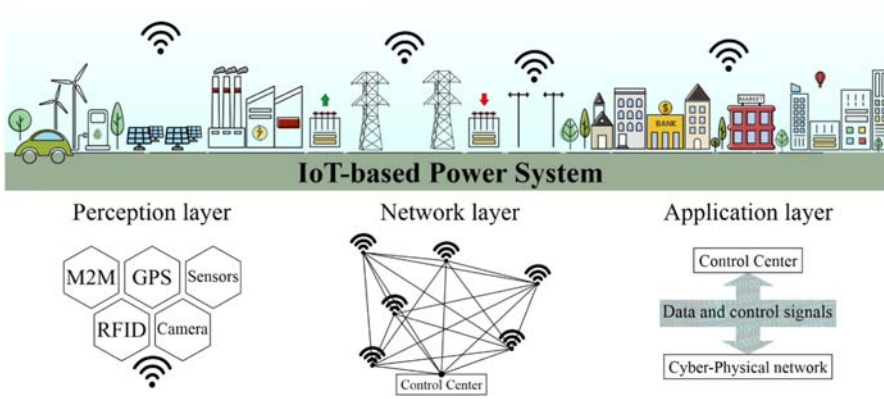


Figure 3.3 IoT-based power system structure layers. *IoT*, Internet of Things.

The IoT-based power systems consist of three main segments, as shown in Fig. 3.3: sensor or perception layer, network layer, and application layer:

3.2.1 Perception (sensor) layer

In the first layer two main objectives, which are sensing and collecting information, should be achieved using a wide range of intelligent and micro-intelligent sensing devices such as radio-frequency identification (RFID), cameras, Global Positioning System, and machine-to-machine (M2M) communication devices. The first layer itself is composed of two sublayers:

- perception control sublayer and
- communication extension sublayer.

The goal of the perception control sublayer is to monitor, control, and acquire data by analyzing the installed IoT devices to realize the perception from the real world. In contrast, the next sublayer can create a connection between IoT devices and the network layer with the help of a communication module.

3.2.2 Network layer

The second layer of the three-layered IoT-based power system is mainly composed of telecommunication networks and the internet. The collected data and information in the perception layer are stored and transmitted in this layer. In the next step, collected data and information are sent to the third layer, the application layer, with the assistance of wireless networks, optical fiber, 5G, and other communication methods. Due to communication between IoT devices, the network protocols play a vital role in information transmission in this layer.

3.2.3 Application layer

This layer is the last section of an IoT-based power system. This layer uses intelligent analysis technology on all of the information and data collected in the network layer to operate power systems more accurately, increase the efficiency of the decision-making, create fault alarms, and monitor remotely. As a result, this layer determines what data is required from which sensor at which time interval to optimize an IoT-based power system operation [22].

3.3 Advantages and opportunities of Internet of Things-based fault monitoring system

IoT brings essential benefits to the SG network. Previously, the use of IoT by humankind in various fields was not prevalent. In recent decades, however, IoT technology has become one of the most vital and inseparable parts of every intelligent network, such as SGs, building management systems, and smart cities. At the broader level, real-time monitoring and control of power networks will lead to better failure diagnosis and be aware of the weaknesses of the system. According to the McKinsey Global Institute, by 2050, the economic impact of IoT on energy and power systems will be approximately 200−500 billion USD [23]. Considering the remarkable penetration of distributed energy resources (DERs), IoT technologies will make the operation, control, and protection of power systems easier. For example, power transmission lines play a crucial role in transmitting the generated power to the distribution network for industrial and residential use. In transmission lines, analog collection of the data generated in remote areas has turned into a pretty challenging task. In contrast, IoT technology for data acquisition has made it easier to access data without considering how far the operators are from the remote data center.

The SG is considered the next generation of power grid, which consists of bidirectional electricity exchange. An intelligent power network is the integration of cyber technologies and communication devices. By connecting DERs to the power grid, the protection methods face a significant challenge. Therefore the possibility of maloperation in the protective devices increases dramatically. For an SG, self-healing is defined as one of the vital characteristics to reduce the downtime of the grid. To achieve this reduced downtime, it is necessary to perform fault positioning initially. Afterward, the self-healing specification can be implemented on the recognized grid asset. With this capability, energy can be transmitted to industrial and residential areas far more efficiently. Furthermore, small energy sectors and independent power producers use IoT to control and monitor their consumption without the help of centralized power systems. In other words, energy sectors have concluded that individually managing the consumption and production will provide a wide range of advantages such as more upgraded security and a better understanding of the microgrids [17].

Since the IoT has got a wide range of applications, it has been widely welcomed by various energy sectors to take advantage of that to control, monitor, gather data,

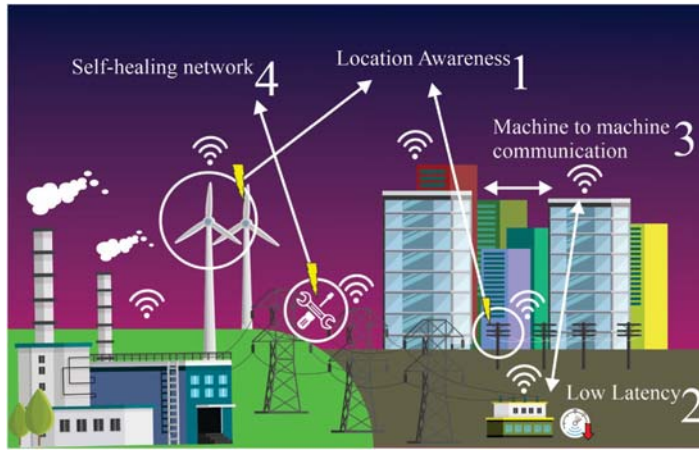


Figure 3.4 Advantages of IoT-based power systems. *IoT*, Internet of Things.

and protect the power grid far more efficiently. IoT technology paves the way for accelerated data analysis using various data collected from different terminals. This technology will lead to fast response services for industrial sectors and end users. A few numbers of advantages of using IoT in SGs are illustrated in Fig. 3.4 and described in the following sections.

3.3.1 Location awareness

Communication and IoT devices are entirely aware of the situation and state of the networks by collecting a tremendous amount of data. Therefore, in case of any failures and fault events, fast and accurate decision-making will be possible with the assistance of the recorded data by the advanced metering infrastructure [24].

3.3.2 Low latency

IoT speeds up the data collecting process even from remote terminals by minimizing human interferences, as gathering the data from remote terminals is quite a challenging task for operators. This is because the data is transmitted to a data center through communication channels. Therefore the access time to the data reduces significantly, assisting the operators in the decision-making process.

3.3.3 Machine-to-machine communication

Intelligent energy systems are implemented in a way that has a complete connection to the IoT devices and exchanges the data between them through these links. In IoT-based power networks, human interference has almost been eliminated. Thus the connection is designed through M2M for monitoring the distribution networks and transmission lines to acquire more efficiency [25].

3.3.4 Self-healing networks

Self-healing power systems are kinds of grids, in which the network problems are resolved without the need for humans to get involved. Network automatic diagnostic and protection tools can detect and remediate outages, failures, and breaches. Self-healing networks provide various benefits:

- cost savings
- real-time fixes without delay
- customer/user satisfaction

3.3.5 Burgeoning renewable energy units' integration

The penetration rate of renewable energy systems (RESs) in the modern power grids has increased since the initiation of climate change countermeasures and policies to decarbonize the electrical industry. However, the usage of IoT-based monitoring devices can be considered another motivation for investments in RESs [26]. This is due to the benefits of IoT systems in monitoring and protecting modern power grids. IoT-based fault positioning systems can communicate wirelessly from remote areas with other sensors and the control center. This option eases the construction of geographically distributed renewable power stations. Also, the presence of IoT-based sensors in the renewable-integrated power systems can provide access to the accurate and real-time data from the grid status, thus enabling automation in the operation of power systems [27]. Additionally, real-time data from the grid status will increase the security of energy supply in the modern power systems, as access to online data will help operators to reduce their decision-making latency or prevent an energy supply-threatening incident to happen.

Moreover, the usage of IoT-based assets for the protection of power systems reduces the overall costs of maintenance and operation in the grid. This issue is important since the sparse positioning of RESs in modern power systems requires extended line construction. Therefore an increase in the investment costs of the grid expansion is inevitable. However, IoT-based monitoring devices will provide useful data from the failures or help the operators to consider preventive actions in the grid [28]. This issue will cause a considerable reduction in the overall maintenance costs that will assist the power system with economic planning for increasing the share of renewable energy in the clean multi-energy mixes. An overview of the impacts of IoT-based monitoring infrastructure on the penetration rate of RESs is presented in Fig. 3.5.

IoT provides limitless prospects for power grid networks which makes the grid interconnected with its up/downstream network altogether [29]. To illustrate, the data is shared by advanced metering devices to exchange information with other nearby/remote metering devices. In this case, the operators will have a clear vision of the system without interfering. For example, whenever the network faced a failure, there was no communication link between the error point and the utility provider before using intelligent monitoring devices. This means that it would take a long time to figure out the accurate location of the fault. After the fault positioning

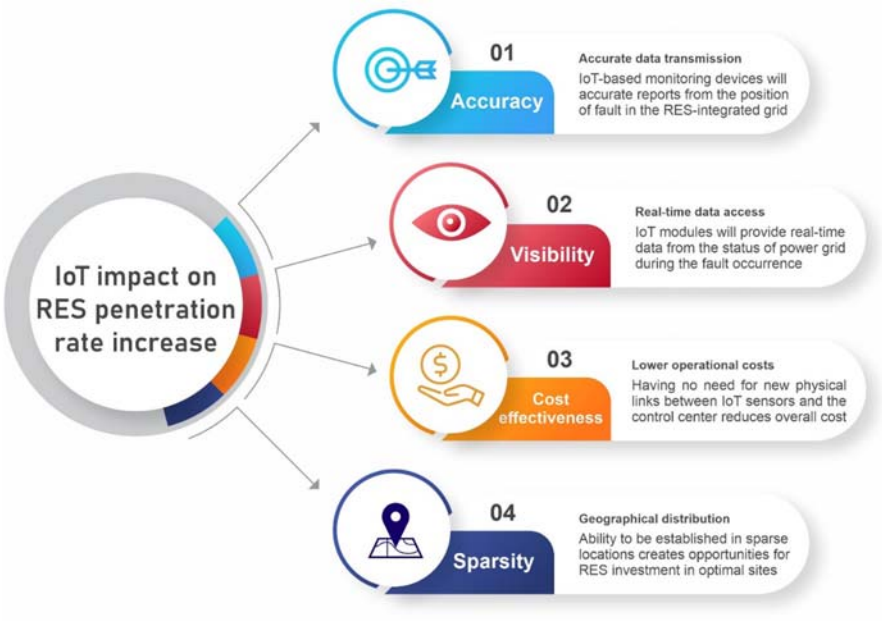


Figure 3.5 Overview of the impacts of IoT-based monitoring infrastructure on the penetration rate of RESs. *IoT*, Internet of Things; *RESs*, renewable energy systems.

was done, the operators could tend to fix the failure by separating the faulted segment of the line for a while, creating an isolated section in the power line. This decision could lead to uncertainty and low reliability. By stark contrast, the gap mentioned above can be shrunk in IoT-based power networks. For instance, before a significant problem occurs, utility providers can be informed about the state of the equipment earlier.

3.4 Challenges of Internet of Things-based fault monitoring system

With the evolution of SG, some emerging technologies are being available commercially to reduce the communication protocols' complexity and quantity, while handling big data in SGs. The IoT is one of the most recent technologies in this field for the SG. Cyberattacks and big data are considered the most crucial challenges in IoT-based SGs and will be discussed generally. Therefore, in case of failure for IoT devices, the reliability of the IoT-based SGs should not be jeopardized. This could be achieved using self-healing and self-organization ability which makes the system develop other alternatives, thereby keeping the whole network under steady-state conditions.

The SG is the design scheme for modern power systems in which IoT-based devices are implemented to ease access to the information of distributed grid assets.

The bidirectional communication network is expanded through the generation, transmission, distribution, and consumption section in SGs. This network expansion eases the operation of SGs while increasing the accuracy of operational decisions. For instance, consumers will be provided with advanced metering devices, power generators will contain smart unit commitment signal devices, and electric transmission and distribution networks will be equipped with various sensors and actuators. The main goal of SGs is to maintain a real-time balance between energy demand and supply by allowing IoT-based devices to perform real-time monitoring, protection, and control over the power system.

The newborn technology called ICT has moved the conventional power system toward a smarter grid. This technology has provided a power system with novel security matters and challenges [30]. Without any doubt, cyber-security is one of the most significant challenges which can be faced by IoT devices. While the use of IoT can provide considerable benefits in the protection and technical security of the SG, it could also lead to catastrophic failures.

Indeed, SG is more attractive for cyber-terrorists as critical infrastructure since its monitoring, protection, and control could be done over standard IoT-based protocols and approaches. Also, the interconnection with public communication infrastructure may generate additional concerns. As a result, an attacker could cause financial losses in the operation of the grid and reduce the resiliency of the grid assets by manipulating the real-time data exchange, which is responsible for the balance between energy demand and supply. This manipulation could be done on the generated data, and signals of the IoT devices or control center. In other words, security plays a vital role in developing reliable IoT-based SGs. Cyber threats can jeopardize the secure operation of the system by disrupting the monitoring and control processes. In general, cyberattacks are divided into the following three categories [31].

3.4.1 Device attack

Device attack mainly concentrates on compromising and taking control of the IoT devices. Attackers initiate the attack by jeopardizing the SG devices to control the whole network. For instance, there is a possibility that a sensor has been modified so that instead of transmitting real-time and accurate data, it sends manipulated and misleading information. As SGs consist of a wide range of interconnected IoT devices, in that case, if one device is affected, it will inject malware into the system. In this case, all parts of the modern power system such as generation, transmission, distribution, and consumption will be infected. As a result, the whole network becomes vulnerable and its reliability will decrease. To overcome this challenge, the operation of all IoT devices should be improved.

3.4.2 Data attack

In terms of data attacks, the main goal is to manipulate, alter, change, and insert data unauthorized or even delete the communication commands to misguide the

intelligent IoT devices of the grid to make wrong decisions which leads to significant problems in the network operation. In general, data attacks happen mainly due to weakness in technology. As the number of communication devices increases and they are getting even more connected than before, there are more places for data to slip through. By using IoT devices and technology without considering the obligatory secure communication protocols, convenience is increasingly valued over security and safety in the operation of IoT-based power systems. Therefore the system will always be vulnerable to security threats. For example, one of the main issues in the monitoring of IoT-based power systems is receiving inaccurate generation data from RESs. This inaccurate dataset can deceive the planning procedure in the power system in a way that they cannot forecast the generation and consumption rates of RESs. Therefore an imbalance between demand and supply can create a contingency event in the operation of the power system, even causing blackouts.

3.4.3 Network attack

Most of the time, network attacks occur in the form of Denial-of-Service (DoS) attacks. A DoS attack can cause outages in the network, barring the access to its vital data for its intended users. DoS attacks accomplish this by flooding the target with cloned and excessive data traffic using the communication channels, which eventually trigger the malfunction in the grid operation. Though DoS attacks do not typically result in the theft or loss of important information or other assets, they can cause the network to lose considerable hardware resources, resulting in increased time for decision-making. Thus it takes the power network operator a while until it verifies the authenticity of the received data. Therefore, in case of any failure in the system, IoT and communication devices will operate with considerable time delay.

Regarding a significant number of "things" such as sensors, RFID, cameras and actuators have made a considerable change in the world. Their strong interactions almost have eliminated the human interference to have an integrated cyber-physical system [32]. On the other hand, each device would collect a wide range of data called "big data." This data includes end users' load demand, power line faults, network components status, scheduling energy consumption, forecast conditions, advanced metering records, outage management records, and a few more [33]. Big data refers to the data that is so large, fast, and complex that makes it considerably time- and hardware-consuming to process using traditional methods. Accessing and storing large amounts of information for analytics has been around for a long time.

It has become a challenging task for IoT-based power systems to acquire, store, analyze, transmit, and secure the generated data [23]. Big data can hand out vital data for the operation of modern power systems by proper analysis. Big data's value does not come from the collection of information. The real value comes from the system's ability to use that stored information to uncover new insights about the state of the network. With big data analytics, it is possible to have an up-to-date, intelligent, and improved power network in all segments (generation, transmission, and distribution). If we want to have IoT-based SGs, various challenges exist regarding big data, which should be considered a significant source of concern.

These hurdles should be addressed because, in case of any failures in the system, they could lead to unpleasant results, especially in transmission and distribution lines, as they are the only way for transmitting energy to different segments. Some of these challenges can be categorized as below [31]:

1. Redundancy reduction and data compression:
   Technically, there exist a wide range of redundant data in the datasets collected from various nearby/remote terminals. Eliminating the iterated data from datasets and reducing their redundancy without threatening the valuable data for the operation of the grid is an important task to do.
2. Data life-cycle management (DLM):

DLM is a policy-based approach that manages the flow of data in an information system throughout its life cycle. This life cycle expands from the creation and initial storage to when it becomes obsolete and is deleted. One of the challenges is that current data centers are not capable of storing a wide range of data. The more up-to-date data a system can host, the more valuable information can be provided to make an appropriate decision in case of failure.

As a result, the acquired data from IoT-based SGs need to be analyzed and processed just like data that requires big data analysis methods [22]. Therefore various collected raw data from different sensing devices should be stored and processed to have real-time monitoring, protection, and control of the SGs.

3.5 Applicability of Internet of Things technology with conventional methods

Technically speaking, the fault current is relatively high during the fault occurrence. Thus the power flow is diverted to the fault, disrupting the power supply of the adjacent zone. In this case, voltage imbalance is inevitable in the power system. Therefore it is critical to identify the problem as soon as possible to prevent irreversible problems in the grid. Many companies that generate and transfer electrical energy via the power grid need to be able to detect different failures such as short circuits on their transmission lines. It is now simple to detect such flaws due to recent improvements in state estimation, fault detection, and positioning technologies. Identifying the relevant fault location was not always straightforward formerly. It was frequently accomplished through the use of specialist organizations tasked with examining transmission lines for faults in a time-consuming procedure [34].

Almost 8 out of 10 outages in the power distribution systems are caused by faults, which result in a loss of system availability. This issue can be considerably improved by speeding up system restoration and minimizing outage length. Also, transmission lines are the most extensively used technical systems for transporting large amounts of electricity between buses in the system [35]. In both of these networks, accurate detection of the failure's location can prevent revenue losses, improve the reliability of the system, and ease access to vital technical parameters

that can be used in maintenance scheduling. As a result, numerous types of fault location approaches are investigated, taking into account the intrinsic characteristics of distribution and transmission lines which can be classified as follows. These approaches are divided into two categories of model-based and data-driven methods [36]:

1. Model-based methods:
   The goal of the model-based techniques is to make sure that the assessed variables are in accordance with the model. Adaptive-based, centralized-based, decentralized-based, differential-based, external device−based, agent-based, local variable−based, traveling wave−based, and transformation/sequence component−based methods are in this category. Specifications, including their advantages and disadvantages, are available in Table 3.1.
2. Data-driven methods:

The basis of these methods is on examination, analysis, and discovery of data and the relationship between various data flow directions of the power system. Usage of decision trees, artificial neural networks, and fuzzy systems in analyzing incoming data from the grid to locate the fault are among the possible data-driven approaches. Specifications, including their advantages and disadvantages, are given in Table 3.1.

Table 3.1 Fault detection and positioning methods.

Method	Explanation	Disadvantages	Resources
Model-based			
Adaptive-based	Examine the updated mode of operation at the relay location whenever the configuration changes. The adaptive protection scheme is applicable for all types of faults in the microgrid system	• Regular readjustment requirements • Calculation complication with the change in the grid topology	[37−40]
Centralized/ decentralized-based	Involves the introduction of Merging Units (MUs) as a synchronized data collector for capturing precise measurements of the instrument.	• The centralized method has higher reliability but longer communication delay • The decentralized method has lower reliability but faster information relaying ability	[41,42]

(*Continued*)

Table 3.1 (Continued)

Method	Explanation	Disadvantages	Resources
Differential-based	The differential current exists only in the case of faults inside the zone	• Lack of backup protection scheme in the case of communication loss	[43–46]
External device–based	An external device is utilized to determine the fault condition of the segmented bus	• Higher capital costs	[47–50]
Agent-based	A computerized system is built of numerous interacting intelligent agents for the protection scheme	• Uncertainty in interagent communications	[51,52]
Local variable–based	Indicating the fault location using the local impedance measurements	• Strong dependency on the grid topology • Higher time delay reduces the performance quality	[53–55]
Traveling wave–based	The internal fault can be identified when the voltage and current traveling waves have opposing polarity on both sides	• Detection is based on high-frequency failures • Vulnerable in front of communication losses	[56,57]
Transformation/ sequence component–based	The fault location is detected using a protection approach based on positive sequence impedance, and the three-phase data retrieved from the PMU is then translated into sequence components	• Requiring fixation of the performance threshold value on the transformation to prevent malfunction in grid	[58,59]
Data-driven			
Decision tree	Defining a decision tree for the protection scheme using the acquired data from the model-based methods	• Need for big data • The complication in decision branch definition • Higher decision uncertainties in interfered grids	[60–62]

(*Continued*)

Table 3.1 (Continued)

Method	Explanation	Disadvantages	Resources
ANN	Forming one or multiple ANNs for the protection scheme to train using acquired data from the model-based methods and locate the failure	• Time-consuming training process • Overfitting and inability in detecting possible relationships within data	[63,64]
Fuzzy	Construct a fuzzy-based decision-making system by defining the membership functions using obtained fault data	• Membership function definition complexity • Requiring testing to ensure sufficient reliability	[65–67]

IoT-based communication technology can be of great assistance for the above-mentioned methods. Covering disadvantages by providing services and positive effects on the grid such as higher reliability, faster communication, reduced capital costs, real-time data presentation, edge computing, and higher observability rates makes IoT technology an attractive option to be implemented in any protection scheme using the methods in Table 3.1.

3.6 The future development path for Internet of Things-based fault detection systems for clean multi-energy mixes

As mentioned in previous sections, IoT-based SG systems are used in power networks in different sections such as monitoring, controlling, and protecting transmission and distribution lines to make them far more intelligent. Therefore providing reliability and availability for communication technologies is of great importance. To make the right decision, communication devices should operate efficiently. Furthermore, self-healing and self-organization are the two vital abilities of IoT-based SGs, which assist the system operation in getting out of abnormal conditions and remaining under stable status [22]. In other words, whenever one of the intelligent IoT devices fails to operate, with the assistance of these capabilities, a new alternative solution must be implemented to prevent the compromising of the system's reliability. To achieve this, various disorders and challenges that IoT-based SGs are facing currently should be addressed in the future.

Batteries are the main power supply of most IoT and communication devices. The online monitoring, control, and protection of power lines in fault positioning applications include various sensors, which operate on batteries in many IoT-based SG systems. It is worth mentioning that batteries can be utilized on longer time scales. Also, their life cycle and deterioration rates can be calculated through multiple methods [68]. To provide power for IoT devices, there is a need to use energy storage resources since their power demand will become one of the main challenges in the short-term future [22]. Developing the electrical energy storage technology to meet sensors' energy demand would result in a breakthrough in electricity transmission and distribution protection, especially in the fault diagnosis of these networks. To achieve this goal, electricity storage devices can manage the amount of power required to supply IoT-based communication devices when needed.

In addition to that, researchers are currently working on one of the critical tasks related to data transmission approaches. To simplify, a significant amount of raw data is transferred between the sensor and the data center. To move this amount of data with higher speed and accuracy, there should be a new generation of communication infrastructures such as 5G and 6G networks between sensors and the data center. Moreover, as IoT-based SGs transfer data based on various wireless nodes, having a proper communication medium in which data can be transferred with high speed is of great significance [29]. For instance, accurate fault data should be transmitted to the data center as quickly as possible to reduce the latency in the decision-making process in transmission and distribution networks. For this purpose, a fast and reliable communication channel should exist to avoid the consequences of delayed performance.

Other future research and open issues can also be considered as a significant source of concern, one of which is that gateway of the communication devices is limited due to functions, considering that only the most necessary data must be selected to be sent and analyzed. Every IoT device has the capability of recording a limited amount of data. It means these devices transmit prespecified data to the data centers. Therefore there should be data fusion technology to integrate the collected raw data by each IoT device. Data fusion means getting data from multiple sources to build more sophisticated models and understand more about the current status of the system. For example, when a fault occurs in transmission or distribution networks, the related data of the failure in the network is not transmitted by a single sensor. Various IoT devices which are distributed in these networks can relay the necessary data about the fault location and its impact on the power system variables such as current and voltage angles. Combining these data will lead to an understandable state report for the operators. In the short-term future, data fusion technology will gain much popularity among researchers to investigate the possible ways to distinguish between necessary and unnecessary data. This will assist power system operation with high-speed operation capability in case of failures in both transmission and distribution networks to provide a secure IoT-based power system.

The IoT has grown so broad that the efforts on the development of its security have to be boosted. While IoT devices play a huge role in the discussion of IoT security, placing all the focus on this aspect does not provide a complete picture of

why protection is necessary and what it entails. However, security is one of the major fields in this regard which requires a deep consideration for researchers in large-scale adoptions [30]. For example, an IoT device can be manipulated so that instead of transferring actual data, erroneous data is sent, and the whole decision-making process is compromised.

3.7 Summary

In this chapter, an overview of IoT technology application in the protection of power networks is discussed. Also, the structure of IoT-based monitoring devices and how they can be implemented in the network are reviewed. The fault location process in transmission and distribution networks was the main focus of this chapter. Transmission and distribution lines are defined as one of the most critical segments of SGs due to their crucial role in transmitting energy. Applying IoT technology makes power systems far more intelligent, and it provides a wide range of opportunities such as M2M communication and self-healing capabilities. However, meanwhile, there exist various challenges and disorders in this regard. One of the main concerns is that IoT-based power systems will be vulnerable in front of different cyberattacks, which can destabilize the whole network. In addition to that, big data is the other challenge that needs to be considered by the researchers as it is getting more and more complex to deal with its presence in modern power systems. As a result, IoT-based power networks require a high-speed communication channel to transfer data, such as 5G and 6G to have reliable protective countermeasures in the SGs. The most remarkable achievements of this chapter are listed below:

- Fault location can be identified far faster and easier with the assistance of various IoT-based devices when compared to traditional fault positioning methods.
- The need for human resources will be minimum as the grid will have the capability to automatically detect the failures and take the proper action.
- Because collecting data from remote terminals is quite difficult, IoT-based power system monitoring schemes make the whole network to be observable by connecting the IoT devices to access data in any given instant.

References

[1] M. El-hajj, A. Fadlallah, M. Chamoun, A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes,", Sensors 19 (5) (2019). Available from: https://doi.org/10.3390/s19051141.

[2] J. Wurm, K. Hoang, O. Arias, A. Sadeghi, Y. Jin, "Security analysis on consumer and industrial IoT devices,", 2016 21st Asia South. Pac. Des. Autom. Conf. (ASP-DAC) (2016) 519–524. Available from: https://doi.org/10.1109/ASPDAC.2016.7428064. 25–28 Jan. 2016.

[3] J. Wu, F. Xiong, C. Li, "Application of Internet of Things and blockchain technologies to improve accounting information quality,", IEEE Access. 7 (2019) 100090−100098. Available from: https://doi.org/10.1109/ACCESS.2019.2930637.

[4] R.V. Yohanandhan, R.M. Elavarasan, R. Pugazhendhi, M. Premkumar, L. Mihet-Popa, V. Terzija, A holistic review on cyber-physical power system (CPPS) testbeds for secure and sustainable electric power grid − Part − II: classification, overview and assessment of CPPS testbeds, Int. J. Electr. Power & Energy Syst. 137 (2022) 107721. Available from: https://doi.org/10.1016/j.ijepes.2021.107721. /05/01/ 2022.

[5] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, "A vision of IoT: applications, challenges, and opportunities with China perspective,", IEEE Internet Things J. 1 (4) (2014) 349−359. Available from: https://doi.org/10.1109/JIOT.2014.2337336.

[6] H. Suo, J. Wan, C. Zou, J. Liu, "Security in the Internet of Things: a review," in: 2012 International Conference on Computer Science and Electronics Engineering, 23−25 March 2012, 3, pp. 648−651. Available from: https://doi.org/10.1109/ICCSEE.2012.373.

[7] K.M.J. Rahman, M.M. Munnee, S. Khan, "Largest blackouts around the world: Trends and data analyses," in: 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), 19−21 Dec. 2016 2016, pp. 155−159. Available from: https://doi.org/10.1109/WIECON-ECE.2016.8009108.

[8] H. Tehzeeb-Ul-Hassan, R. Zafar, S.A. Mohsin, O. Lateef, Reduction in power transmission loss using fully informed particle swarm optimization, Int. J. Electr. Power & Energy Syst. 43 (1) (2012) 364−368. Available from: https://doi.org/10.1016/j.ijepes.2012.05.028. /12/01/ 2012.

[9] D.P. Nedic, I. Dobson, D.S. Kirschen, B.A. Carreras, V.E. Lynch, Criticality in a cascading failure blackout model, Int. J. Electr. Power & Energy Syst. 28 (9) (2006) 627−633. Available from: https://doi.org/10.1016/j.ijepes.2006.03.006. /11/01/ 2006.

[10] A. Wang, Y. Luo, G. Tu, P. Liu, "Vulnerability assessment scheme for power system transmission networks based on the fault chain theory,", IEEE Trans. Power Syst. 26 (1) (2011) 442−450. Available from: https://doi.org/10.1109/TPWRS.2010.2052291.

[11] L. Hua, Z. Junguo, L. Fantao, "Internet of things technology and its applications in smart grid,", TELKOMNIKA Indonesian J. Electr. Eng. 12 (2) (2014) 940−946.

[12] J.A. Jiang, H.C. Chiu, Y.C. Yang, J.C. Wang, C.H. Lee, C.Y. Chou, "On real-time detection of line sags in overhead power grids using an IoT-based monitoring system: theoretical basis, system implementation, and long-term field verification,", IEEE Internet Things J. (2021). Available from: https://doi.org/10.1109/JIOT.2021.3139933. 1-1.

[13] J. Fallah Ardashir, H. Vatankhah Ghadim, Introduction and literature review of cost-saving characteristics of multi-carrier energy networks, in: M. Nazari-Heris, S. Asadi, B. Mohammadi-Ivatloo (Eds.), Planning and Operation of Multi-Carrier Energy *Networks*, Springer International Publishing, Cham, 2021, pp. 1−37.

[14] J. Fallah Ardashir, H. Vatankhah Ghadim, Chapter 14 - Large-scale energy storages in joint energy and ancillary multimarkets, in: B. Mohammadi-Ivatloo, A. Mohammadpour Shotorbani, A. Anvari-Moghaddam (Eds.), Energy Storage in Energy Markets, Academic Press, 2021, pp. 265−285.

[15] J.F. Ardashir, H.V. Ghadim, A PV based multilevel inverter with ultra-capacitor bank for microgrid applications, 2021 11th Smart Grid Conference (SGC), 2021, pp. 1−5. IEEE.

[16] L.d. Andrade, T.P.d. Leão, Impedance-based fault location analysis for transmission lines, PES. T&D 2012 (2012) 1−6. Available from: https://doi.org/10.1109/TDC.2012.6281527. 7−10 May 2012.

[17] P. Kumar, S. Nikolovski, Z.Y. Dong (Eds.), Internet of Energy Handbook (1st ed.), CRC Press, 2021.
[18] X. Kong, Y. Xu, Z. Jiao, D. Dong, X. Yuan, S. Li, "Fault location technology for power system based on information about the Power Internet of Things,", IEEE Trans. Ind. Inform. 16 (10) (2020) 6682–6692. Available from: https://doi.org/10.1109/TII.2019.2960440.
[19] S. Abhishek, G.A. Abhinav, M. Abhishek Kumar, S. Pushpa Mala, Transmission lines management system for smart grids, in: 2020 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), 26–27 December 2020, IEEE, 2020, pp. 44–47.
[20] W. Li, J. Su, X. Wang, J. Li, Q. Ai, Fault location of distribution networks based on multi-source information, Glob. Energy Interconnect. 3 (1) (2020) 76–84. Available from: https://doi.org/10.1016/j.gloei.2020.03.005. /02/01/ 2020.
[21] A. Bahmanyar et al., "Fast fault location for fast restoration of smart electrical distribution grids," in: 2016 IEEE International Smart Cities Conference (ISC2), 12–15 Sept. 2016 2016, pp. 1–6. Available from: https://doi.org/10.1109/ISC2.2016.7580741.
[22] Y. Saleem, N. Crespi, M.H. Rehmani, R. Copeland, "Internet of Things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions,", IEEE Access. 7 (2019) 62962–63003. Available from: https://doi.org/10.1109/ACCESS.2019.2913984.
[23] G. Bedi, G.K. Venayagamoorthy, R. Singh, R.R. Brooks, K.C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems,", IEEE Internet Things J. 5 (2) (2018) 847–870. Available from: https://doi.org/10.1109/JIOT.2018.2802704.
[24] S. Chen, et al., "Internet of Things based smart grids supported by intelligent edge computing,", IEEE Access. 7 (2019) 74089–74102. Available from: https://doi.org/10.1109/ACCESS.2019.2920488.
[25] R. Bikmetov, M.Y.A. Raja, T.U. Sane, "Infrastructure and applications of Internet of Things in smart grids: a survey," in: 2017 North American Power Symposium (NAPS), 17–19 September 2017, pp. 1–6. Available from: https://doi.org/10.1109/NAPS.2017.8107283.
[26] N. Hossein Motlagh, M. Mohammadrezaei, J. Hunt, B. Zakeri, "Internet of Things (IoT) and the energy sector,", Energies 13 (2) (2020). Available from: https://doi.org/10.3390/en13020494.
[27] S. Ponnalagarsamy, V. Geetha, M. Pushpavalli, P. Abirami, "Impact of IoT on renew energy,", IoT Appl. Comput. (2022) 107.
[28] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, L. Patrono, Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future, J. Clean. Prod. 274 (2020) 122877. Available from: https://doi.org/10.1016/j.jclepro.2020.122877. 2020/11/20/.
[29] S.S. Reka, T. Dragicevic, Future effectual role of energy delivery: a comprehensive review of Internet of Things and smart grid, Renew. Sustain. Energy Rev. 91 (2018) 90–108. Available from: https://doi.org/10.1016/j.rser.2018.03.089. 2018/08/01/.
[30] C. Bekara, Security issues and challenges for the IoT-based smart grid, Procedia Computer Sci. 34 (2014) 532–537. Available from: https://doi.org/10.1016/j.procs.2014.07.064. 2014/01/01/.
[31] H. Hu, Y. Wen, T.S. Chua, X. Li, "Toward scalable systems for big data analytics: a technology tutorial,", IEEE Access. 2 (2014) 652–687. Available from: https://doi.org/10.1109/ACCESS.2014.2332453.
[32] R. Atat, L. Liu, J. Wu, G. Li, C. Ye, Y. Yang, "Big data meet cyber-physical systems: a panoramic survey,", IEEE Access. 6 (2018) 73603–73636. Available from: https://doi.org/10.1109/ACCESS.2018.2878681.

[33] M. Jaradat, M. Jarrah, A. Bousselham, Y. Jararweh, M. Al-Ayyoub, The Internet of Energy: smart sensor networks and big data management for smart grid, Procedia Computer Sci. 56 (2015) 592−597. Available from: https://doi.org/10.1016/j.procs.2015.07.250. 2015/01/01/.

[34] B. Godavarthi, V.D. Majety, Y. Mrudula, P. Nalajala, "Fault identification in power lines using GSM and IoT technology," in: First International Conference on Artificial Intelligence and Cognitive Computing, Singapore, R. S. Bapi, K. S. Rao, M. V. N. K. Prasad, (Eds.), 2019: Springer Singapore, pp. 647−655.

[35] A. Sauhats, A. Jonins, V. Chuvychin, M. Danilova, "Fault location algorithms for power transmission lines based on Monte-Carlo method," in: 2001 IEEE Porto Power Tech Proceedings (Cat. No.01EX502), 10−13 September 2001, 3, p. 5 pp. vol.3. Available from: https://doi.org/10.1109/PTC.2001.964900.

[36] M. Shafiullah, M.A. Abido, A review on distribution grid fault location techniques, Electr. Power Compon. Syst. 45 (8) (2017) 807−824. Available from: https://doi.org/10.1080/15325008.2017.1310772. 2017/05/09.

[37] K.-Y. Lien, et al., "A novel fault protection system using communication-assisted digital relays for AC microgrids having a multiple grounding system, Int. J. Electr. Power & Energy Syst. 78 (2016) 600−625. Available from: https://doi.org/10.1016/j.ijepes.2015.12.019. 2016/06/01/.

[38] O.V.G. Swathika, S. Hemamalini, "Prims-aided Dijkstra algorithm for adaptive protection in microgrids,", IEEE J. Emerg. Sel. Top. Power Electron. 4 (4) (2016) 1279−1286. Available from: https://doi.org/10.1109/JESTPE.2016.2581986.

[39] H. Muda, P. Jena, "Superimposed adaptive sequence current based microgrid protection: a new technique,", IEEE Trans. Power Delivery 32 (2) (2017) 757−767. Available from: https://doi.org/10.1109/TPWRD.2016.2601921.

[40] A.R. Haron, A. Mohamed, H. Shareef, H. Zayandehroodi, "Analysis and solutions of overcurrent protection issues in a microgrid," in: 2012 IEEE International Conference on Power and Energy (PECon), 2−5 December 2012, pp. 644−649. Available from: https://doi.org/10.1109/PECon.2012.6450293.

[41] C. Yuan, K. Lai, M.S. Illindala, M.A. Haj-ahmed, A.S. Khalsa, "Multilayered protection strategy for developing community microgrids in village distribution systems,", IEEE Trans. Power Delivery 32 (1) (2017) 495−503. Available from: https://doi.org/10.1109/TPWRD.2016.2544923.

[42] M. Monadi, C. Gavriluta, A. Luna, J.I. Candela, P. Rodriguez, "Centralized protection strategy for medium voltage DC microgrids,", IEEE Trans. Power Delivery 32 (1) (2017) 430−440. Available from: https://doi.org/10.1109/TPWRD.2016.2600278.

[43] Z. Akhtar, M.A. Saqib, Microgrids formed by renewable energy integration into power grids pose electrical protection challenges, Renew. Energy 99 (2016) 148−157. Available from: https://doi.org/10.1016/j.renene.2016.06.053. 2016/12/01/.

[44] C. Yuan, M.A. Haj-ahmed, M.S. Illindala, "Protection strategies for medium-voltage direct-current microgrid at a remote area mine site,", IEEE Trans. Ind. Appl. 51 (4) (2015) 2846−2853. Available from: https://doi.org/10.1109/TIA.2015.2391441.

[45] S. Dhar, P.K. Dash, "Differential current-based fault protection with adaptive threshold for multiple PV-based DC microgrid,", IET Renew. Power Gener. 11 (6) (2017) 778−790.

[46] A. Gururani, S.R. Mohanty, J.C. Mohanta, "Microgrid protection using Hilbert−Huang transform based-differential scheme,", IET Generation, Transm. & Distrib. 10 (15) (2016) 3707−3716.

[47] S. Choi, A.P.S. Meliopoulos, "Effective real-time operation and protection scheme of microgrids using distributed dynamic state estimation,", IEEE Trans. Power Delivery 32 (1) (2017) 504–514. Available from: https://doi.org/10.1109/TPWRD.2016.2580638.

[48] R. Kheirollahi, E. Dehghanpour, "Developing a new fault location topology for DC microgrid systems," in: 2016 7th Power Electronics and Drive Systems Technologies Conference (PEDSTC), 16–18 February 2016, pp. 297–301. Available from: https://doi.org/10.1109/PEDSTC.2016.7556877.

[49] K. Lai, M.S. Illindala, M.A. Haj-ahmed, "Comprehensive protection strategy for an islanded microgrid using intelligent relays," in: 2015 IEEE Industry Applications Society Annual Meeting, 18–22 October 2015, pp. 1–11. Available from: https://doi.org/10.1109/IAS.2015.7356952.

[50] M.H. Cintuglu, T. Ma, O.A. Mohammed, "Protection of autonomous microgrids using agent-based distributed communication, IEEE Trans. Power Delivery 32 (1) (2017) 351–360. Available from: https://doi.org/10.1109/TPWRD.2016.2551368.

[51] H.F. Habib, T. Youssef, M.H. Cintuglu, O.A. Mohammed, "Multi-agent-based technique for fault location, isolation, and service restoration, IEEE Trans. Ind. Appl. 53 (3) (2017) 1841–1851. Available from: https://doi.org/10.1109/TIA.2017.2671427.

[52] A. Hussain, M. Aslam, S.M. Arif, N-version programming-based protection scheme for microgrids: A multi-agent system based approach, Sustain. Energy, Grids Netw. 6 (2016) 35–45. Available from: https://doi.org/10.1016/j.segan.2016.02.001. 2016/06/01/.

[53] F. Ferdowsi, H. Vahedi, C.S. Edrington, "High impedance fault detection utilizing real-time complexity measurement," in: 2017 IEEE Texas Power and Energy Conference (TPEC), 9–10 February 2017, pp. 1–5. Available from: https://doi.org/10.1109/TPEC.2017.7868289.

[54] S. Chae, J. Park, S. Oh, "Series DC arc fault detection algorithm for DC microgrids using relative magnitude comparison,", IEEE J. Emerg. Sel. Top. Power Electron. 4 (4) (2016) 1270–1278. Available from: https://doi.org/10.1109/JESTPE.2016.2592186.

[55] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, W. Tian, "Protection scheme for loop-based microgrids,", IEEE Trans. Smart Grid 8 (3) (2017) 1340–1349. Available from: https://doi.org/10.1109/TSG.2016.2626791.

[56] X. Li, A. Dyśko, G.M. Burt, "Traveling wave-based protection scheme for inverter-dominated microgrid using mathematical morphology,", IEEE Trans. Smart Grid 5 (5) (2014) 2211–2218. Available from: https://doi.org/10.1109/TSG.2014.2320365.

[57] M.A. Aftab, S.M.S. Hussain, I. Ali, T.S. Ustun, Dynamic protection of power systems with high penetration of renewables: a review of the traveling wave based fault location techniques, Int. J. Electr. Power & Energy Syst. 114 (2020) 105410. Available from: https://doi.org/10.1016/j.ijepes.2019.105410. 2020/01/01/.

[58] S. Beheshtaein, M. Savaghebi, J.C. Vasquez, J.M. Guerrero, "A hybrid algorithm for fault locating in looped microgrids," in: 2016 IEEE Energy Conversion Congress and Exposition (ECCE), 18–22 September 2016, pp. 1–6. Available from: https://doi.org/10.1109/ECCE.2016.7855166.

[59] S. Mirsaeidi, D.M. Said, M.W. Mustafa, M.H. Habibuddin, "A protection strategy for micro-grids based on positive-sequence component,", IET Renew. Power Gener. 9 (6) (2015) 600–609.

[60] S. Kar, S.R. Samantaray, M.D. Zadeh, Data-Mining Model Based Intelligent Differential Microgrid Protection Scheme, IEEE Syst. J. 11 (2) (2017) 1161–1169. Available from: https://doi.org/10.1109/JSYST.2014.2380432.

[61] S. Kar, S.R. Samantaray, "Data-mining based comprehensive primary and backup protection scheme for micro-grid," in: 2015 IEEE Power, Communication and Information Technology Conference (PCITC), 15−17 October 2015, pp. 505−510. Available from: https://doi.org/10.1109/PCITC.2015.7438217.

[62] D.P. Mishra, S.R. Samantaray, G. Joos, "A combined wavelet and data-mining based intelligent protection scheme for microgrid,", IEEE Trans. Smart Grid 7 (5) (2016) 2295−2304. Available from: https://doi.org/10.1109/TSG.2015.2487501.

[63] Q. Yang, J. Li, S. Le Blond, C. Wang, Artificial neural network based fault detection and fault location in the DC microgrid, Energy Procedia 103 (2016) 129−134. Available from: https://doi.org/10.1016/j.egypro.2016.11.261. 2016/12/01/.

[64] D.K.J.S. Jayamaha, N.W.A. Lidula, A.D. Rajapakse, "Wavelet-multi resolution analysis based ANN architecture for fault detection and localization in DC microgrids,", IEEE Access. 7 (2019) 145371−145384. Available from: https://doi.org/10.1109/ACCESS.2019.2945397.

[65] A.S.F. Sobrinho, R.A. Flauzino, L.H.B. Liboni, E.C.M. Costa, Proposal of a fuzzy-based PMU for detection and classification of disturbances in power distribution networks, Int. J. Electr. Power & Energy Syst. 94 (2018) 27−40. Available from: https://doi.org/10.1016/j.ijepes.2017.06.023. 2018/01/01/.

[66] M. Dehghani, M.H. Khooban, T. Niknam, Fast fault detection and classification based on a combination of wavelet singular entropy theory and fuzzy logic in distribution lines in the presence of distributed generations, Int. J. Electr. Power & Energy Syst. 78 (2016) 455−462. Available from: https://doi.org/10.1016/j.ijepes.2015.11.048. 2016/06/01/.

[67] A.H. Abdulwahid, W. Shaorong, "A new protection approach for microgrid based upon combined ANFIS with Symmetrical Components," in: 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), 25−28 October 2016, pp. 1984−1989. Available from: https://doi.org/10.1109/APPEEC.2016.7779851.

[68] J. Steiner, M. Blakeley, A. Miller, "Estimating the battery life of a wireless occupancy sensor,", Lutron Electron. Co., Inc. IP. (2014) 367−2437.

Architecture and applications of Internet of Things in smart grids

4

Saman Ghanbari[1], *Saeed Yadegari*[2] *and Mohsen Kalantar*[1]
[1]Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran, [2]Department of Electrical Engineering, Razi University, Kermanshah, Iran

Chapter Outline

4.1 Introduction

The Internet of Things (IoT) is a new and exciting technology that has the potential to alter the global by connecting physical things. With the launch of the first application for automated inventory systems in 1983 [1], the concept of IoT as a collection of heterogeneous smart devices became real. However, it took off as a promising technology for the internet's future vision in 1999 [2]. Today, the rising scarcity of tiny and affordable computer devices with detection and communication capabilities is paving the road for IoT perception everywhere. IoT provides an interconnected connection to everyday objects. All physical items on the Earth (such as appliances, products, buildings, cars, and plants) are referred to as "Things" in the "Internet of Things". It was predicted that by 2020, IoT would be associated with roughly 50 billion smart devices, which will be more than six times the world's expected population, making it one of the fastest growing technologies in all computing. Though IoT consequences are prevalent, the smart link is with present networks, with information sensing by computers conducted without the help of human participation. IoT implementations are being expanded into various

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00011-2

applications such as households, industries, energy systems, logistics, cities, agriculture, and health care [3].

Electricity is a requirement that significantly influences our contemporary civilization and the worldwide community. However, the majority of power system architecture was created more than 50 years ago, has grown complicated, and cannot meet the needs of today's contemporary civilization [4]. The incorporation of IoT technology into power systems can successfully integrate and increase the information level, power infrastructure usage, and device interaction facilities as well as promote advanced information and communication system services within the power grid system. In addition, since there is such a wide variety of devices, energy forms with their intrinsic behavior, the variation of specific parameters in the energy field, and the unpredictability of certain phenomena, large volumes of data must be sent and analyzed in near real time, and choices must be taken with little delay. The data should be transferred to the correct destinations quickly and securely, and the needed actions should be carried out automatically. Consequently, the solution is to outfit individual components with technologies geared toward IoT so that they may utilize networks of information technology. Electric boards are included in IoT-based products that include microprocessors and can transfer information, such as sensors, meters, or controllers [5]. These boards are also known as "Internet of Things" boards. In addition, the veracity and accuracy of the information must be ensured, both of which might be jeopardized by intentional or unintentional cyberattacks or interruptions [6].

So, based on the importance of IoT in power system, different researchers have paid special attention to this concept in recent years. For instance, in Ref. [7], a review about IoT applications in smart grid (SG) was proposed. In Ref. [8], low-cost smart meters for the applications of IoT in SGs were discussed. In Ref. [9], improving the security of SGs using capability of IoT was presented. In Ref. [10], a review about using IoT in demand response of SGs was presented. So, these papers and many similar ones show the importance of using IoT in SGs. Therefore, in this chapter, some applications of IoT in SGs will be introduced.

4.2 Internet of Things in smart grid

The IoT helps to solve some of the problems hindering the development of SG. These problems include the tracking and connectivity of a large number of SG devices as well as the collaboration that is required between these devices via ubiquitous, distributed, and autonomous communications. As a result, IoT technologies would be capable of creating, facilitating, and accelerating the overall developments in the SG by providing support for various network operations inside the grid. Utilizing the IoT technologies in the power industry typically consists of three fundamental steps, the first of which is digitizing the assets, the second of which is collecting the asset data, and the third of which is developing computational algorithms in the control systems. In this context, communications infrastructures

must have a guaranteed Quality of Service and comply with industrial standards and particular security needs in the SG. Fig. 4.1 illustrates an element of the IoT that will be discussed in more depth in the following sections.

4.3 Internet of Things in generation level

Historically, the generation resource management was managed via local regulating devices. Since the system operator has limited controllability of remote control, many activities have to be carried out by sending orders or instructions to be done by a local operator. This is necessary because of the nature of the system. In addition, the management of generating assets in power systems is becoming more complicated than it has ever been for various reasons. Besides, there is an increase in the penetration of renewable energy resources, which significantly contributes to the unpredictability of power networks. Electric cars will become more prevalent shortly, affecting the power grid generation schedule. Third, the engagement of loads as demand response resources is growing, closely related to the volatile hourly power prices. The price of electricity is also tied to numerous other factors, including the structure of the power market and the price of immediate fuel. Furthermore, demand-side medium-scale or small-scale distributed generation (DG), also known as virtual power plant, or microsources will be widely used soon. The operator should cope with such a high level of unpredictability in the network, in addition to current grid limits, which might result in load shedding in different situations. To avoid such actions and maintain security, stability, dependability, and environmental sustainability of the power system, IoT technology may help with issue solving and problem-solving. In IoT-enabled SGs, all fluctuations and

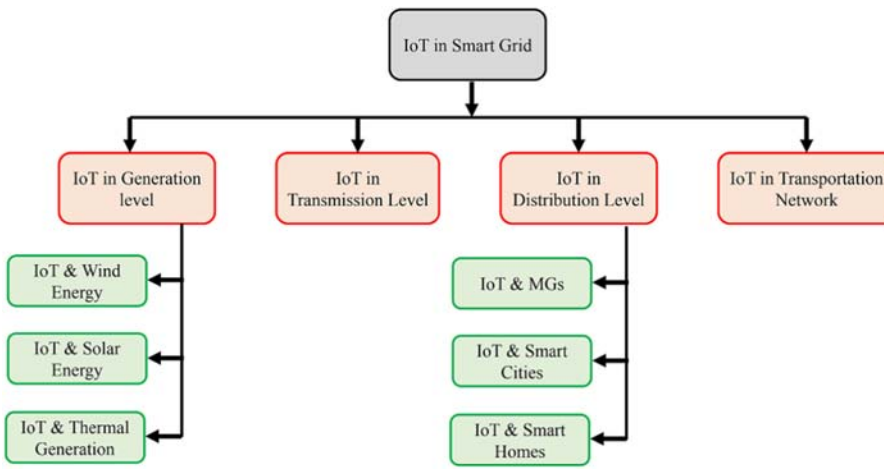


Figure 4.1 Different aspects of IoT in smart grid. *IoT*, Internet of Things.

generations on both the demand and supply sides can be automatically and precisely monitored, allowing the operator to have more sophisticated grid supervision. The combination of a few energy resources such as nuclear, oil, coal, and hydro as well as renewable energy sources such as geothermal, solar, wind, and marine-based energies is the focus of IoT technologies at the generation level, in order to improve the performance of the generation sector and maintain the dynamic and static security of the power system. Furthermore, energy storage utilities may be used to correct imbalances created by various sources of uncertainty that IoT networks might alter. Notion of IoT has been mostly centered on the demand side, with little emphasis on the supply side. Because of a greater degree of controllability and observability, deployment of IoT at this level may lead to better efficiency and performance, bringing enormous advantages to power systems. A comprehensive schematic of using IoT in generation level is presented in Fig. 4.2.

4.3.1 Internet of Things and wind energy

Wind energy has seen rapid growth in terms of installed capacity worldwide. By 2014 worldwide wind energy output had surpassed 369 GW, with more than 51 GW of new capacity 2014, reflecting a 16% growth rate. China had the most

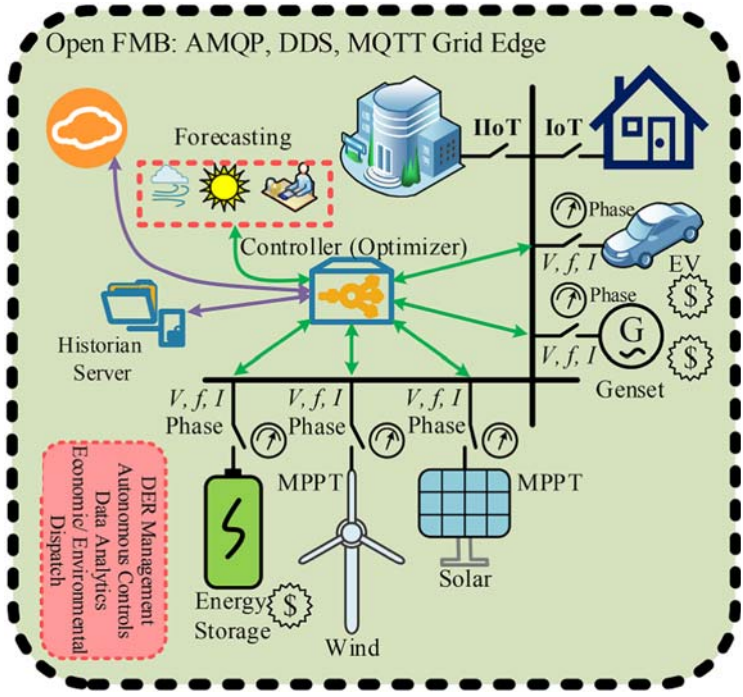


Figure 4.2 Implementation of IoT for generation level [6]. *IoT*, Internet of Things.

installed capacity in 2014, with 23.4 GW, Germany had 5.3 GW, the United States had 4.9 GW, Brazil had 2.5 GW, and India had 2.3 GW. Denmark has set a new global record with 39% of total energy output from wind power. Other nations with a high wind percentage of energy generation include Spain (21%), Portugal (20%), Ireland (16%), and Germany (9%) [11]. Wind energy deployment objectives for the future are lofty. Wind energy's global expansion necessitates technology breakthroughs such as floating, offshore, large-scale, and flying wind turbines. The deployment of these systems underscores the need for more strict and comprehensive procedures for designing, installing, operating, and maintaining safe, secure, and cost-effective frameworks. Wind energy has significant hurdles due to the stochastic nature of the wind power generation, including fluctuations and unwanted dynamic changes in captured power. Furthermore, a wind turbine amid strong turbulence may suffer detrimental consequences such as fatigue and excessive stress. As a result, wind turbine control systems are mainly concerned with capturing energy at the lowest possible cost, that is, to allow efficient energy production with specific power characteristics while reducing loads to extend the turbine's life span and decrease maintenance costs. These goals need complicated and efficient management systems [12].

The energy businesses are confronting various issues due to rising energy consumption and a limited supply of fossil fuels. These issues need the development of novel technologies for effective and dispersed energy generation, management, and consumption. For instance, in intelligent coal mines and oil fields, ubiquitous sensors with pervasive and real-time computing are used. In terms of wind energy, modern wind energy conversion system (WECS) designs are shifting from centralized and traditional structures to decentralized, distributed, and more complicated systems to meet varying energy production needs, consumer demands, and environmental fluctuations. Utility-scale wind turbines are becoming more extensive, while wind farms span wider regions and increase attention in distant and offshore places. Furthermore, wind energy produces varying amounts of electricity, necessitating modern power electronics and energy storage devices [13]. As a result of the rising complexity of WECS and the management of interactions and coordination between components, more comprehensive and systematic techniques are required. Furthermore, a wind turbine amid strong turbulence may suffer detrimental consequences such as fatigue and excessive stress. As a result, wind turbine control systems are mainly concerned with capturing energy at the lowest possible cost. That is, to allow efficient energy production with specific power characteristics while reducing loads to extend the turbine's lifespan and decrease maintenance costs. These goals need complicated and efficient management systems [14].

A wind turbine is made up of several major components, including the yaw system, tower and foundation structure, blades, rotor hub, pitch system, drive shaft, high-speed shaft, brake system, gearbox, generator, power converter, wind sensor, nacelle, transformer, and central controller. The controller layer is densely packed with sensors and actuators. The sensors may report each intrinsic component's health and performance. The control system is responsible for regulating and manipulating the components. It does this by using a set of actuators. The five

layers of sensors are temperature (bearings, oils, windings, and electronic components); environmental (humidity, wind speed, ice, and illumination); mechanical (speeds, positions, stresses, angles, and strain); electrical (current, voltages, frequencies, power factors, and faults); and fluid sensors. The environmental sensors measure things such as ice and wind speed (pressure, levels, flow). The controller is responsible for providing electric, hydraulic, and mechanical commands and instructions and receiving sensor data via power amplifiers [13].

Consequently, cyber-physical devices are needed to link the physical layer of wind turbines to the cyber layer by means of network architecture. The cyber layer comprises the network, the system of condition monitoring, and the supervisory control and data acquisition (SCADA) system. A network is a dependable connection that enables the transmission of control signals and data between a controller. Additionally, a network provides for the connectivity of intelligent equipment and devices that are deeply buried inside a wind farm. The network's primary purpose is to simplify the transfer of control signals and data in real time between the controller, supervisory center, sensors, actuators, and data storage stations. In particular, the local circumstances significantly impact the architecture of the communication network used in offshore wind farms. Installing what is known as a remote terminal unit, or RTU, on each wind turbine is necessary to establish a connection to a local area network (LAN). A LAN is linked to a condition-monitoring system (CMS) at both the wind farm and turbine levels. This is done to allow control of wind turbines and simplify earlier fault detection to stop cascading failures of wind turbines in a wind farm caused by voltage dips. In addition, an SCADA system is also linked to all of these monitoring systems.

As a consequence, CMS can maintain its stability by using one of three different methods: under-voltage ride through, fault ride through, and low-voltage ride through. These systems function in conjunction with a centralized data center to spread the data via a wide area network hosted in the cloud. All wind farm turbines are integrated with distributed intelligence devices and embedded systems based on the IoT and use wireless sensor networks. Furthermore, these turbines are equipped with machine-to-machine (M2M) communication with a cloud-based network that sends data to servers through internet-enabled and open communication protocols. Last but not least, these turbines can be operated and monitored through unified computer-aided interfaces or mobile human−machine interfaces (HMIs). It is hypothesized that the IoT-based controlling system will have a heftier price tag than the standard SCADA systems in use today; nevertheless, it will have a greater capacity for diagnosis due to a higher information frequency and a higher sample rate. IEC 61400-25 is a standard developed to execute unified monitoring and information sharing. Within this standard, the autonomy, diagnostics, extensibility, and standardization of the data exchange gateway are enhanced [15].

4.3.2 Internet of Things and solar energy

One of the most important forms of renewable energy now available is solar photovoltaic, or PV, energy. Solar power is emerging as a viable option for meeting the

need for sustainable energy sources in the years to come. There is a growing demand for monitoring of real-time generation data obtained from solar PV plants to optimize the overall performance of the solar power plant and maintain the grid's stability as more and more rooftop solar PV systems are getting integrated into the existing grid. This is necessary in order to keep the grid stable. Because the installation cannot carry out local monitoring, monitoring from a distant location is an absolute need for any solar power plant [16].

Solar panels, sometimes known as PV arrays, wiring, switches, mounting system, and inventors, are the primary components of a PV system. A battery storage unit is an option that may be paired with these accessories (battery bank). New technologies, such as global positioning system (GPS) solar trackers, maximum power point tracker (MPPT) controlling schemes, solar radiation sensors, and anemometers, are incorporated into today's PV systems to facilitate the more effective collection of solar power. Concentrator photovoltaics (CPV) are solar panels that, in contrast to traditional PV systems, are outfitted with optical lenses and curved mirrors. These components work together to assist in concentrating sunlight onto a multijunction solar cell that is very small but very efficient. In addition, a cooling system is often included in CPVs to increase their overall efficiency. Both PV and solar power work best in areas with high average irradiation. Due it has considerably smaller capital cost per kW, traditional PV systems may also be employed for DG, such as building-integrated solar output or rooftop-mounted. This is possible because of the systems' flexibility. Currently, many PV systems are grid-connected rather than self-contained. The generation power of PV systems primarily depends on the surrounding environment's temperature and the amount of sunshine radiation. It is important to remember that the performance of the PV system may be significantly worsened by shade and dirt, which can lead to a significant decrease in output power. In addition, if the temperature rises, the PV system's efficiency will decrease, which is a significant drawback. The Maximum Power Point Tracking (MPPT) technology will tilt the panel to either face the sun head-on or the brightest portion of the sky when it is partially cloudy. It is essential to have a storage facility because solar electricity has to be stored at all times when it is available, and the storage facility has to be able to supply the energy that has been saved when it is required [17].

Changes in sun irradiation, temperature, and other conditions may impact the amount of electricity solar PV plants generate. Therefore remote monitoring is essential. IoT is an approach that is being taken to develop a remote monitoring system for solar PV power plants. This approach envisions a near future where commonplace objects will be equipped with microcontrollers and transceivers for digital communication. IoT-based systems take a giant leap toward monitoring by intelligent decision-making from the web, which is made possible by the elimination of risks associated with traditional wiring systems, which are eliminated by the use of remote monitoring, which also makes the process of data measurement and monitoring much simpler and more cost-effective. The remote monitoring system's decentralized design and deployment flexibility make it ideal for use in industrial settings [18].

4.3.3 Internet of Things and thermal generation

Thermal power plants are essential to the world's current power generation infrastructure. The functioning of the grid is made more reliable and resilient because of the presence of these kinds of devices. However, to reduce their environmental impact, conventional thermal power plants are being phased out in favor of renewable resources in future power systems. They are also characterized by poor levels of efficiency and adaptability in their operations. Currently, gas-fired generators are included in the category of costly generating units. Because of these factors, there will likely be the least amount of deployment of IoT technology in this area of the electrical grid compared to other aspects. However, IoT function's importance might come from two different aspects. At first, the state of the transformers and tap changers, the status of the generators, and the power through each branch need to be precisely presented to the system's control center. Therefore the architecture of the IoT might make retrieving data in real time more straightforward. In addition, traditional steam power plants have a diverse assortment of parts and features in their construction. To schedule preventive maintenance and overhauls, which reduce the risk of unplanned outages, the engineers at the power plant must ensure that the current state of health is automatically recorded and monitored by using advanced sensors based on the IoT [6].

4.4 Internet of Things in transmission level

The transmission level sits between the generating and distribution levels, acting as a link between the two. This level is an essential component of the power systems that must be present to guarantee a steady supply of demand. Integration of IoT technologies at the transmission level is significant for two reasons. The first is the influence that IoT will have on the continued upkeep of system security, and the second will be the consequence that IoT will have on the development of congestion management. Intelligent electronic devices that are equipped with the IoT technology may be deployed in the transmission sector to provide information to the operator about the electrical status of the lines, such as losses and disruptions. Phasor measurement units, also known as PMUs, use the GPS to keep their time synchronized, enabling them to calculate the magnitude and angle of the voltage and current at a particular point along the line. Additionally, this apparatus can differentiate the frequency. A commercial version of the PMU can provide readings with a high temporal resolution at around 30−60 measurements per second. Because of this issue, power system engineers are given the ability to do dynamic event analysis inside the power system. A measurement that is both so quick and exact would be impossible to take with typical SCADA systems, which only communicate their results once every 2 or 4 seconds. In conjunction with the protective relays, the protective monitoring units (PMU) may be used to implement the wide-area protection systems. The development of microsynchronous PMUs that use a non-GPS reference time calibration has made it possible to report 120 samples per

second, which assists in preventing catastrophic blackouts. PMUs can offer data with a high degree of accuracy to display both the active and reactive power traveling through the line. This increases the visibility of the system. Because of this issue, preventive and astute control activities and techniques have been developed. The operator can automatically control congestion in crowded power networks or locally congested regions thanks to the monitoring of real-time power through the lines. This is especially helpful in the event of crises and other unanticipated circumstances. As a consequence, the operator's degree of mobility may be boosted. In addition, overhead cables are susceptible to damage from natural catastrophes. Strong winds and extreme snowy conditions may produce galloping and freezing of power lines, all of which can result in an uneven pulling force to the wires, which can cause towers to lean over. Damage to the overhead wires is incurred due to these variables, increasing operational risk. In addition, the transmission system is dispersed over a large region of land, making it difficult to maintain and monitor in certain areas due to its isolation. The use of IoT can potentially reduce the amount of harm caused by such natural occurrences. It is necessary to collect the relevant data using sophisticated sensing devices mounted atop the conductor or towers of the transmission line. The data must first be sent to the device that serves as the sync node, and then it must be transmitted to the central command and control center via either an optical fiber network or wireless communication channels.

4.5 Internet of Things in distribution level

When energy storage equipment, electric vehicles, large-scale DG, electric vehicles, and flexible loads gain high-density access to the distribution network, the distribution network shifts from the passive network used in the past to the active network with power flowing in both directions. The introduction of multiple dynamic, active components at the distribution level, such as energy storage equipment, distributed energy resources (DERs), electric vehicles, and flexible loads, lead to new challenges to the system stability, particularly regarding power quality, voltage regulation, and the dependability of the grid. Therefore the active distribution network (ADN) technology offers viable solutions to the abovementioned issues. With the help of this technology, the conventional passive mode of operation of the distribution network may be replaced with the active management and control that is performed by the current state of operation of the grid [19].

In light of what was just discussed, it is essential to look at practical ways to enhance one's knowledge of the current operational condition of the distribution network. To provide active control and management of distribution networks, the construction of distributed monitoring systems can provide vast amounts of real-time information. This information can include the current operating state of DERs, energy storage equipment, and flexible loads, amongst other things. This sort of observability in space may be realized with the help of a distributed monitoring system based on the IoT technology. In addition, because of the unpredictability and

volatility risk involved in the functioning of distribution networks, it is essential to improve the observability of situation awareness on a temporal scale. It is possible to use situation awareness technology to accomplish the change from passive treatment to active prevention as well as to master the operating situation of a distribution network in real time and analyze the trend of the future scenario. As a result, developing a distributed monitoring system for ADN and investigating situation awareness technologies are necessary steps toward achieving space-time panoramic situation awareness and early warning.

4.5.1 Internet of Things in microgrids

The management of energy in a microgrid has to be carried out in a manner that is separate from the main network. On microsources, the main network has no control and can make no observations. The operator of the microgrid is the one who is responsible for making projections about unreliable microsources. The internal storage unit is responsible for restoring equilibrium after the imbalances it has caused. However, because such systems have restricted abilities in terms of resiliency, the operator of microgrid is required to implement unplanned and undesirable load shedding. The introduction of IoT into interconnected microgrids enhances the controllability and observability of the operator of main grid on microgrid components. It enables the operator to consider the characteristics of all microsources to generate the whole system. Because of this issue, there will be an increase in the penetration of renewable energy resources and an improvement in the functioning of the power system. Also, the operator of microgrid can improve the cooperation between renewable energy sources and storage facilities, which may raise the microgrid's profitability in the real-time pricing of the power market. Also, real-time monitoring is beneficial to the regulating schemes since it helps to get higher quality electricity. In addition, if two or more microgrids are linked, their scales' incompatibility might affect the system's joint stability. As a result, the safety of the others may be jeopardized by even a somewhat severe imbalance in any one of them. In this context, the incorporation of real-time frequency and voltage stability regulating systems is necessary to satisfy the demand continuously. Because of this topic, it is necessary to use an environment based on the internet and IoT infrastructure. The data must be obtained from all of the sensors for the controlling devices to be informed of the real-time condition of the essential parameters. The data must be processed by utilizing cloud computing, and the appropriate action has to be chosen by following the prespecified instructions [20].

4.5.2 Internet of Things in smart cities and homes

In the past, the demand pattern was considered a random process guided by statistical laws. Today, however, this view has changed. As a result, the professionals working in the power business and the planners must utilize complex procedures to adjust the generation to the demand in real time. As a result of this lack of demand management, excessive expenses were paid since the grid size was intended for

peak transmission. Due to the nature of this situation, it is necessary to create a significant amount of generating capacity that will only be used for a few hours each year. As a result, the concept of encouraging higher levels of demand in exchange for lower levels of consumption via incentives or penalties was established. This notion eventually developed into what we now know as demand response due to its success. Customers were encouraged to sign voluntary or mandatorily contracts that were understood to represent a particular form of demand response program (DRP). DRPs may be broken down into two categories: incentive-based programs and time-based rate programs (TBR). The term "time-based rate" refers to the pricing strategy for energy that encourages a response from the user owing to the immediate price. Real-time pricing, also known as RTP, time-of-use pricing, often known as TOU pricing, and critical peak pricing comprise TBR. These systems incentivize consumers to demonstrate a sensitive reaction associated with the price of electricity at the moment [21].

When seen from the point of view of the operator, demand response resources, which are also referred to as DRRs, are conceptualized in the same manner as a virtual demand-side power plant. In today's world, operators frequently allow DRRs that are more reliable as an alternative to calling in an expensive unit during peak hours. This is because calling in a unit can be expensive. After the establishment of power markets and the beginning of the process of reorganizing power systems, the concept of demand response arose as a potential solution to the problem. The restructuring and deregulatory policies put into place brought about a change in how electrical networks operate.

Nevertheless, the incorporation of advanced metering infrastructures that are fitted with IoT connection technologies has the potential to be a big step forward toward another shift. At this present moment, people all around the world are seeing a shift toward a more significant digital presence in their day-to-day lives. Some DRPs may be carried out on an impromptu basis by end users, in addition to the automated demand response for home appliances or gadgets discussed before. Therefore, by incorporating an IoT-based communication infrastructure, end users can have a more convenient level of control over a wide variety of devices and pieces of equipment by employing computer-based interfaces or HMIs such as mobiles and tablets. This is possible because of the benefits discussed previously. A comprehensive schematic of using IoT in smart homes is presented in Fig. 4.3.

4.6 Internet of Things in transportation networks

As the IoT continues to develop, more and more apps that aim to improve people's lives are being created. Cities are becoming "smarter," and apps designed specifically for smart cities are being created to use the most recent technological advances. The development of intelligent transportation systems is made possible by the IoT arrival in the realm of transportation, which enables transportation systems to "feel" and "think" for the first time [22]. Because there are plenty of

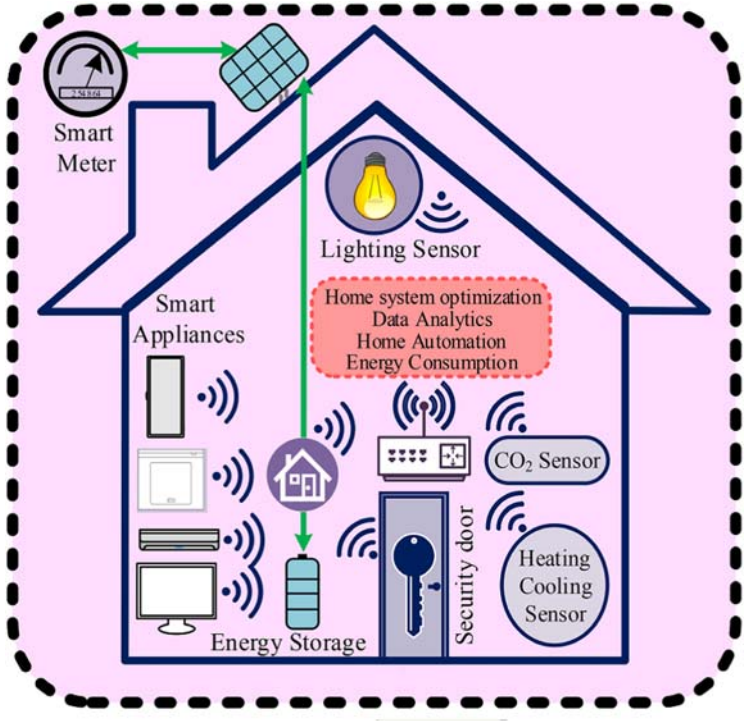


Figure 4.3 Implementation of IoT for a smart home [6]. *IoT*, Internet of Things.

chances for additional improvements, intelligent transportation has garnered the attention of many researchers. Navigation and optimizing travel routes are two critical topics of interest in smart transportation. Applications try to estimate traffic congestion using data from users' mobile devices [23] or side units placed in specific locations on the road [24]. These applications also propose optimal route options to minimize travel times, reducing the amount of energy consumed by cars and the emissions they produce.

In addition, to promote the decrease in energy usage, it is recommended to install street lights capable of detecting the current traffic circumstances and operating appropriately, as opposed to always being on according to a predetermined timetable. The IoT has also been widely used to create intelligent parking systems. Researchers have proposed new parking reservation systems using cameras [25] or other wireless sensors such as a magnetic field or infrared [26]. These systems allow for the availability and capacity of a parking lot to be maximized while simultaneously reducing the amount of time spent searching. In addition, there have been suggestions made for systems that may assist with detecting irregularities in the road surface by using input data from sensors mounted to vehicles or carried by the driver on their phone. Accidents may be averted if poor road conditions can be identified and reported in time. There have also been attempts to use IoT devices to

identify or avoid vehicular accidents. Last but not least, the IoT M2M communication option has made it possible to develop vehicle-to-vehicle communication and vehicle social networks. In these networks, individual vehicles can communicate with one another to share relevant information and open up a wide variety of new application possibilities [27].

4.7 Summary

This chapter studied the use of the IoT in different aspects of SGs. The findings of the research were separated into four main areas. The first part of this chapter described the implications of the IoT on the generation level, in which the necessity of innovation corresponding with solar and wind resources and thermal plant facilities has been explained. The next part represents the transmission layer. The IoT in this layer enhances the observability of lines, ultimately leading to improved monitoring of the transmission grid. Therefore the operation will be more secure, and better emergency congestion management will be possible with integrated controllers with autonomous IoT technology. The following part was about distribution network, in which an investigation was conducted into the function that the IoT plays in distribution networks, microgrids, smart cities, smart buildings, and smart homes. Finally, the last part presented the implementation of IoT in transportation networks.

References

[1] M. Weiser, The computer for the 21st century, IEEE Pervasive Comput. 1 (1) (2002) 19–25.
[2] J. Pontin, ETC: Bill Joy's Six Webs, MIT Technology Review, 2005.
[3] J. Tao, et al., The impact of Internet of Things supported by emerging 5G in power systems: a review, CSEE J. Power Energy Syst. 6 (2) (2019) 344–352.
[4] A. Ghasempour, Internet of things in smart grid: architecture, applications, services, key technologies, and challenges, Inventions 4 (1) (2019) 22.
[5] G. Bedi, et al., Review of Internet of Things (IoT) in electric power and energy systems, IEEE Internet Things J. 5 (2) (2018) 847–870.
[6] H. Shahinzadeh, et al. "IoT architecture for smart grids." in: 2019 International Conference on Protection and Automation of Power System (IPAPS), IEEE, 2019.
[7] R. Pal, et al., A comprehensive review on IoT-based infrastructure for smart grid applications, IET Renew. power Gener. 15 (16) (2021) 3761–3776.
[8] M. Orlando, et al., A smart meter infrastructure for smart grid IoT applications, IEEE Internet Things J. (2021).
[9] R. Borgaonkar, et al., Improving smart grid security through 5G enabled IoT and edge computing, Concurrency Computation: Pract. Experience 33 (18) (2021) e6466.
[10] S. Ahmadzadeh, G. Parr, W. Zhao, A review on communication aspects of demand response management for future 5G IoT-based smart grids, IEEE Access. 9 (2021) 77555–77571.

[11] World Wind Energy Association. “Key statistics of world wind energy report 2013.” Shanghai, 7 April 2014.
[12] M. Mohammed, A. Mahmoud Moustafa, A survey of cyber-physical advances and challenges of wind energy conversion systems: prospects for internet of energy, IEEE Internet Things J. 3 (2) (2015) 134−145.
[13] R. Rajkumar, et al. “Cyber-physical systems: the next computing revolution.” in: Design automation conference. IEEE, 2010.
[14] F. Kong, et al. “Quantity versus quality: Optimal harvesting wind power for the smart grid.” in: Proceedings of the IEEE 102.11, 2014, pp. 1762−1776.
[15] F. Al-Turjman, M. Abujubbeh, IoT-enabled smart grid via SM: an overview, Future Gener. Computer Syst. 96 (2019) 579−590.
[16] S. Constantin, et al. “GPRS based system for atmospheric pollution monitoring and warning.” in: 2006 IEEE International Conference on Automation, Quality and Testing, Robotics. Vol. 2. IEEE, 2006.
[17] A.S. Spanias. “Solar energy management as an Internet of Things (IoT) application.” in: 2017 8th International Conference on Information, Intelligence, Systems & Applications (IISA). IEEE, 2017.
[18] S. Adhya, et al. “An IoT based smart solar photovoltaic remote monitoring and control unit.” in: 2016 2nd International Conference on Control, Instrumentation, Energy & Communication (CIEC). IEEE, 2016.
[19] L. Chen, et al. “Construction and application research of active distribution network situation awareness system.” in: 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC). IEEE, 2016.
[20] M. Moazzami, et al. “Application of multi-objective grey wolf algorithm on energy management of microgrids with techno-economic and environmental considerations.” in: 2018 3rd Conference on Swarm Intelligence and Evolutionary Computation (CSIEC). IEEE, 2018.
[21] A. Abdollahi, et al., Investigation of economic and environmental-driven demand response measures incorporating UC, IEEE Trans. smart grid 3 (1) (2011) 12−25.
[22] F. Zantalis, et al., A review of machine learning and IoT in smart transportation, Future Internet 11 (4) (2019) 94.
[23] J. Yang, et al., Optimization of real-time traffic network assignment based on IoT data using DBN and clustering model in smart city, Future Gener. Computer Syst. 108 (2020) 976−986.
[24] A. Al-Dweik, et al. “IoT-based multifunctional scalable real-time enhanced road side unit for intelligent transportation systems.” in: 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE). IEEE, 2017.
[25] Q. Wu, et al. “Robust parking space detection considering inter-space correlation.” 2007 IEEE international conference on multimedia and expo. IEEE, 2007.
[26] A. Araújo, et al., IoT-based smart parking for smart cities, IEEE First Summer School on Smart Cities (S3C), 2017, IEEE, 2017.
[27] B. Jain, et al., A cross layer protocol for traffic management in Social Internet of Vehicles, Future Gener. Computer Syst. 82 (2018) 707−714.

Artificial intelligence–enabled Internet of Things technologies in modern energy grids

5

Arman Behnam[1], *Sasan Azad*[2,3], *Mohammadreza Daneshvar*[4], *Amjad Anvari-Moghaddam*[5] *and Mousa Marzband*[6,7]

[1]Department of Computer Science, Illinois Institute of Technology, Chicago, United States, [2]Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran, [3]Electrical Networks Research Institute, Shahid Beheshti University, Tehran, Iran, [4]Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, [5]Department of Energy (AAU Energy), Aalborg University, Aalborg, Denmark, [6]Electrical Power and Control Systems Research Group, Northumbria University, Newcastle upon Tyne, United Kingdom, [7]Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah, Saudi Arabia

Chapter Outline

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00004-5

5.1 Introduction

Throughout time, state-of-the-art technologies are changing the industrial and energy environments. Specifically, in artificial intelligence (AI)-based technologies in the connectivity area, the most popular application is mainly Internet of Things (IoT) and its settings implementation. New AI-based methods help with the computation and analytical power needed in modern energy grids. Hence, we will delve into IoT knowledge to facilitate the process.

IoT process generally is categorized into (1) Internet technologies usage and smart objects interconnection, (2) Likewise internet services, aiding in technologies batch are required to find out the perceptions, such as radio-frequency identifications (RFID), sensors, switches, actuators, and machine-to-machine (M2M) connection devices, and (3) service and application layers influencing such technologies to trigger new grid's business opportunities. Since only one frequent Internet protocol (IP)-based digital network in the IoT is available, different networks such as home area network (HAN), wide area network, and neighborhood area network (NAN) are not necessarily used [1]. All the subdepartments in the industry retain help from an IP-based network by service providers in their applications layer. The recent approach is the communication networks' architecture incentive that reduces time and smoothens the path for capital investment reallocation. The first main smart grid (SG)'s deployment component is the smart meter that gives access to smart metering setup at dwelling units, profit-making sector, and industrial users [1].

In this chapter, a new approach for IoT technologies in SGs is discussed. This new approach looks at these technologies as an object that contains features, including infrastructure, components, challenges, future structure, and applications. There are some combinations of these features discussed in this chapter, such as the role of new IoT technologies in SGs and Energy Internet, which are AI-enabled IoT technologies.

5.1.1 Internet of Things basics in smart grids

Modern power networks are being introduced as SGs. Some key problems of the current electric power system are one-orientation information, spoiled energy, flourishing energy demand, and reliability. In modern power grids, it is vital to implement operations and analytics in a new way that stands on employing AI-based technologies on the IoT platform. There are many important tasks in these grids, including data gathering, data preprocessing, data processing, data analytics, and reaching results. Each of these tasks is considered in modern energy grids' tasks with regard to its challenges.

Computing integration and bidirectional communication potential with current power infrastructures happen in SG. All energy value chain levels are considered, which are not restricted to smart metering (SM). In addition, intelligent use of sensors, embedded computing, and digital communications make the electricity network discernible (measurement and visualization scope), controllable (manipulation

and optimization scope), automated (adaptive and self-correcting), and fully integrated (full interoperability with current systems and being able to incorporate a wide energy source span) [2]. So, a complete SG requires IoT devices connectivity, automation, and real-time monitoring. A vast range of network functions throughout the generation, transmission, distribution, and power consumption are supported in SG systems by the IoT devices integration [2].

5.1.2 The relationships between Internet of Things and intelligent grids

An SG creates a cross-directional data platform for optimal monitoring of the system and efficient energy supply by AI technologies network. In an intelligent grid, end users are able to determine the demand by data collection via an IoT network. IoT helps with battery management and monitoring, causing the minimizing of the unnecessary waste demand by electricity supply [3].

The prospective view of IoT facilitated SGs is not determined with the virtual connection considering all utility providers to customers. The interconnection that contains smart phones data becomes possible with data-driven decision-making through collaboration comprising IoT reduction in application total cost of ownership. In the past, since no communication between the user and utility provider was available, a failing transformer had a poor supply. The smart meters and sensors used for data extraction provide complete information for triggering the process. This is the basics of a compressive work order generation. When a blackout happens, a notification by the power line sensor is sent to utility providers where the transformer action is being monitored. This instant action is accomplished more gently, making an efficient wireless system by IoT [4].

5.1.3 Internet of Things in power systems

IoT is mostly used in the distribution and consumption power sector. According to Fig. 5.1, in the third and fourth layers, IoT and the system's operator control the interactions with power distribution and consumption.

A power flow example is explained by Fig. 5.2, which is the complement of Fig. 5.1. A step-by-step power development process and IoT usage are shown in Fig. 5.2. Because of the urgent alert in the power system operation and control center in the moment of failure in transformers, IoT is a crucial problem in SGs. With the approach of power saving, SGs try to solve the power consumption problem with the help of IoT, since the process is monitored on a momentary basis in the data center. The outcome is efficient power saving with an active scheduling approach.

The modern SGs have interconnected elements with built-in preservation and intelligence. Because of the need in utilizing substitute energy resources, service providers are no longer dependent on the customers. IoT is completely adjusting the energy zone with the largest chain added value. Hence, inferential data analytics

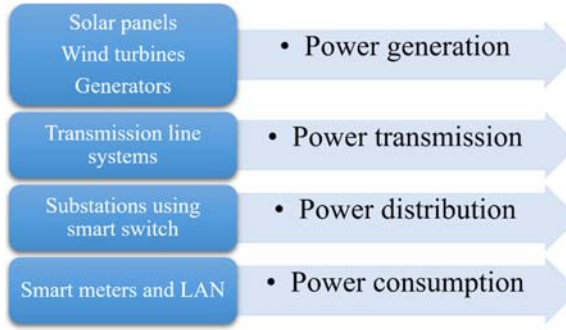


Figure 5.1 IoT in power systems. *IoT*, Internet of Things.

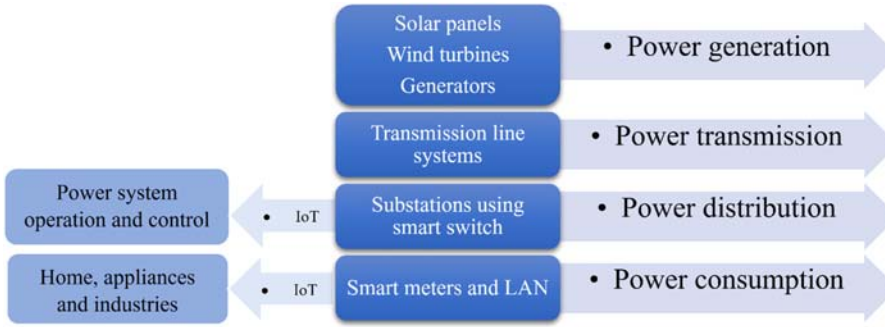


Figure 5.2 General power flow systems.

is suitable using for the collected dataset and the other real-time equipment results in pivotal insight toward settled business decisions that have become transcendent [4].

5.1.4 Smart grid roles and drawbacks in power systems

Smart grid (SG) is basically defined as a smart automated electric grid, including a batch of computers and services [5]. Based on the load type in use and energy systems network (ESN) type (e.g., residential, operational, monetary, and industrial), differences will be obvious in services. The present SG framework is associated with several structure scenarios, which change based on the operational range. Some of these operations such as energy-dependent smart cities output, energy-based residential operations computing systems, and energy conservation blueprints enabled by metering and tracing processes [5]. SG technologies and device utilization can substantially reduce renewable energy resources (RER) problems and allow SGs to effectively use the potential of RERs for clean energy production. Accomplishing complete SG is significant for the distributed energy resources (DER) efficiency. It is also important to provide electricity management (demand/supply) between

renewable energy (RE) technologies and energy storage systems (ESSs) with attention to both electricity consumers and producers [6].

Despite SGs having many positive effects to help the industry in many ways, there are also drawbacks to triggering such a system. First, the overhead costs of an SG are extremely expensive and time-consuming and cause labor costs increasing; however, this will result in creating many jobs in the new market for electricity. Second, the privacy standards violation which is possible according to continuous data usage. This internet-based system usage could lead to security issues. Some of the problems are acquainted with the trend of SG technology installation.

One of the main SG's goals is promising peer's active attendance with mechanized bonds. Data-driven decisions are vital for a distributed energy distribution network that has a bidirectional electricity flow with the associated data. Besides residential, economic, and industrial loads, SG also helps with a combined operation for electric vehicle (EV) charging structures. As a matter of fact, SGs gather all the electrical system production, transmission, and consumption architecture together, so the overall system performance will be improved for the sake of customers and the IoT ecosystem. In general, the SG strengthens ESN operation and the context of generation, transmission, and distribution management and decision-making [7].

Conversion to SG fundamentals from traditional grids, including digital energy vision and its devices deployment, can be gradual and piecemeal. The related process will be started by running a small prototype project as a nanogrid, mini-grid, or microgrid remotely. The SG implementation drawback shows the interest of the provider and the consumer, bolstered by third-party regulatory restrictions and technological standards hindering SG solutions [8].

While designing SG, concerns such as ensuring reliability, resiliency, security, computational, and the SG operations' energy efficiency in the digitalization process become vital. Fast, modern computing methods and digital tools such as AI, IoT, big data analytics, machine learning (ML), deep learning (DL), cloud computing, and blockchain have been rationally applied in building administration, transportation, networking, and manufacturing to build sustainable and energy-efficient systems.

With new technologic devices and emerging algorithms, enabling data-driven decisions will help with the quotes below, which will be discussed in the chapter [8]:

- An introduction to DER, power electronics components, communication and cybersecurity issues in SG.
- The techniques associated with AI, such as fuzzy logic, knowledge-based systems, artificial neural networks, and their roles in distributed energy-based SGs.
- Energy Internet architecture, including the IoT components.
- The AI-based analysis has the potential to enhance SG services.
- The IoT and blockchain services, such as data collection, data storage, and digital transactions among the associates within ESN and its groups, are accomplished.
- Automated services to associates are achieved by the ESN's real-time extracted knowledge from data for monitoring, authenticity, accessibility, flexibility, strength, security, and viability purposes.

5.2 Communication infrastructure

After a brief knowledge of the different aspects of IoT in SGs, information about the infrastructures, including networks, electrical components, etc., needs to be investigated.

5.2.1 Smart grid internet infrastructure

The SG Architecture Model framework is introduced as an SG applications reference architecture and contains specifically five main interoperability layers, employment, functions, information, communications, and elements. Different aspects of SG and its services, operations, assets, and devices are addressed by one layer in the power grid's functionality support. Four interconnected sectors aggregate the communication infrastructure of SG, including the backbone network, the middle-mile network, the last-mile network, and the premises area network (PAN) [9]. Each of the sectors' functionality is discussed as follows:

- The backbone network supporting the link between the diverse subsystems and the public utility sites.
- The backhaul network conveys data flow to the advanced metering infrastructure (AMI) with mechanized distribution in architecture and public utilities operation control centers. The network explains an efficient evaluation focusing on its utilization and application [10].
- Moreover, the communication in SG networks progresses considering operational and sensorial data structure, which must be adjustable and consecutive. Hence, the network might be managed by operators and employ wireless technologies such as wireless fidelity (Wi-Fi), Worldwide Interoperability for Microwave Access, and mobile networks such as long-term evolution (LTE) and 5G [10].
- The last-mile network: Supporting by NAN, FAN, and AMI, which facilitates the smart energy meters' data gathering and their propagation to concentrators [10].
- The PAN: It is implemented by HANs, based on programmable logic controller (PLC) standards. The HAN adjusts several elements, such as lighting control, basement automation, thermostats, heating, ventilation and air conditioning, and plug-in hybrid electric vehicle/electric vehicle [10].

Cellular technology has been progressive with one goal, which is new industry enhancement. With the arrival of low-power wide-area network technologies, the IoT paradigm's integration in a an SG design is being discussed among the experts.

5.2.2 Power electronic components

The relationship between the power grid and DERs is an essential function in the SG system performance, which introduces the role of power electronics. Furthermore, boosting, regulation, and DC/DC or DC/AC transformation electricity, especially grid and RE integration, happens in this process. For interfacing to the grid, the distributed energy unregulated RE sources' voltage output and intermittency require power electronics [11].

The DER's voltage output has two states: DC and AC, which comes into the calculations with variable frequency. Power electronics, such as high-voltage direct current, voltage source inverter, and boost converter, grant grids additional supplies with the goal of improving power excellence, reactive power service, and electric grid strength and balance. A smart inverter that merges RE and ESS technologies to the electric grid, has the ability to serve distinctive operations to make a power system performance more stable and reliable [12].

5.2.2.1 Volt-VAR control

The definition of Volt-VAR control is the responsive power injection for voltage regulation. Smart inverters have the ability to provide reactive power for the discussed goal at connection points for the SG voltage regulation. An Inverter special design and program cause its reactive power output to be dependent on the grid voltage.

A communication link is employed to utilize the power converter. It is another solution for the injection process by the grid operator command. In the interfacing meantime, the inverter is able to monitor variables, including current, voltage, frequency, and phase angles, with regard to control functions. This extracted information will further be used for data analytics and data-driven actions [13].

5.2.2.2 Ramp-rate control

Nontransmissible RE, such as solar and wind production outputs, fluctuates many times, even in a few minutes, which might cause confusion for the operators. A reduction in the up/down output power ramping rate is possible with a smart inverter associated with a built-in supercapacitor [14].

5.2.2.3 Frequency and voltage

If the RE production output parameters such as voltage and frequency are not within an acceptable range, the inverter is not able to release the output into the grid. However, there may be an exceptional temporary period of low/high voltage or frequency on the grid. If renewable sources have a further loss, the situation might aggravate these grid conditions [15].

5.2.3 Communication challenge and cyber-security

Assuring effective communication among the peers is an important matter in SGs. Also, protection should be implemented on the SG operations' database. On this subject, the communication role and assured cyber-security systems are discussed below.

5.2.3.1 Communication role in smart grid

The bidirectional information flow, electricity flow, and real-time communication between elements in the system is a vital problem in SGs. Communication

importance comes up with two challenges; first, grid integration with DER, and second, aid in the reconstruction of the ESN topology according to the electric power adjustment need. Since SG is a large and complicated system, it needs a range of cutting-edge network technologies that can enable high-speed bidirectional intercommunication among elements, users, and operators in a specific time interval. Usually, these communications are wired (power line communication, fiber optics, and copper cables) optionally. Also, there are other wireless communications, such as Wi-Fi, cellular, and microwave. [16].

In the traditional grids' approach, engineers use power sensors as input for data collection and a consumer's terminal for the monitoring process, which takes place on a regular timetable basis. While in SGs, smart meters and sensors/devices receive real-time data and store all historical data by remote monitoring. All this extracted grid information is the output of an interaction platform connecting to a central processing unit with all considered points using wired/wireless communication technologies. This new real-time condition monitoring notices IoT power systems' operators about devices' health status by AI-based prediction, so they will be informed about the fault occurring ahead of time. This information includes variables such as notifications on possible outages with duration, energy consumption from the power meter, and available energy in determined time intervals. Additionally, users have the option to alter their power consumption patterns extracted from information available in the power databases in accordance with their power consumption rate and total cost. When IoT layers are completed in SG, this information and changing ability is accessible on an exchanging information platform [17].

5.2.3.2 Cyber-security role in smart grid

A need to prohibit misuse, suspicious destructive activities, and unauthorized access to an SG's bidirectional information flow is considered as a reason for cybersecurity in SG. Great consumption knowledge as an output of information analytics and consumers' commerce patterns are available within ESN. So, the data has to be protected from leakage, being hacked, and loss.

Inadequate cyber-security standards will expose the IoT system to a high-risk cyberattack, which compromises the IoT system and face our grid with stability challenges. Other problems such as fraud, information leakage, energy consumption, and collected data manipulation are outcomes of cyberattack. Cyber-security must be interpreted as accessibility, cohesion, creditability, and data accessibility schedule. Moreover, cyberattacks and information security violations detection in SGs will be solved by automatically sending signals to the peer. As a result, the peer will be helped in protecting the system cohesion [18].

5.2.4 Internet of Things components

The data preprocessing transmission for the SGs are categorized into an information and implementation database. The output results consist of smart meter results

readings, utility statements, power consumption rates, power flow patterns, and customers' geographical information system (GIS) in SG. The SG's performance data contains a condenser bank, fault positions, IoT network's ongoing variables levels, and energy storage statistics [19]. The central and incidental technologies employ distinctive intelligent devices mentioned below:

5.2.4.1 Advanced sensing and intelligent measurement system

SM arises with the data gathering process on energy prices and resource usage rates. This includes the electricity consuming time and quantity. System security, SG integration with upcoming technologies, and state-of-the-art protective support in SGs all allow the customer to alleviate grid congestion. Grid stability improvement through early faults detection occurs through advance monitoring and analysis, helps in operating system isolation, and prevents power outages [19].

5.2.4.2 Mechanized monitoring and control

Real-time energy tracking for power device status display is a great SG feature, which takes place by optimization power system modules, device operators, and user recognition. These technologies extract data and supply a visual system status presentation for the decision-making process and help to enhance power distribution scope and authenticity [20].

5.2.4.3 Renewable resources consuming prediction

There is a need for an accurate forecast according to the intermittent nature of REs, specifically wind and solar. Advanced precise energy accessibility computations can lessen negative effects on the SG's required spinning reserves. Furthermore, it will contain exploratory knowledge on utilities, load, and other vital computational SG factors. A dynamic nature in all power system type levels, while equalizing the generating variables process, interprets forecasting by stabilizing the grid [21].

5.2.4.4 Information and communication technology

What is typical in current power system base includes all significant power system operational facilities (power generation, transmission, and primary distribution substation) connecting to the control unit center. However, extended communication taking place throughout power delivery networks ends in offering express bidirectional information flows. This forms the SG into a dynamic state for real-time communication. SGs employ information and communication technologies according to the power system status with attention to the up-down nature of a generation. Its goal is to perform more effectively for consumer appliances. Hence, electric power maintenance, grid dependability and productivity, cost-benefit analysis, and environmental protection will be improved [22].

5.2.4.5 Power distribution industrialization

Distribution automation (DA) is a method for mechanized control for power distribution networks' efficiency maximization, so the SG will be more steady and well-performed. As an important SG element, it enables the distribution geographical location readjustment to integrate RE mutability, power increasing, and two-way power flows. The DA facilitates voltage and power factors sensing and monitoring at some determined points on the power distribution circuit. In case of deviation detection from the determined feasible range, it causes voltage regulating devices automated control. So, the reflexive power and voltage injection to be regulated to the present value is allowed. In the moment of fault, the fault's real-time moments can be identified and located faster and more accurately by operators, even at remote locations. So, the time wasted on manual fault tracking will be reduced, and consumers/users do not see the troubleshooting time as a problem anymore [23].

5.3 Key features in energy internet

With the socioeconomic growth influence in mind, it is a noticeable practice to determine linked uncertainties affecting the energy demand/supply patterns. So, satisfactory, reliable, flexible, equal, and secured energy supplies exploration is preferred the most. Concerning environmental protection, and other clean energy standards in the energy supplies, efficient and viable energy resources are commanded to make socioeconomic growth secure. Considering DER, particularly RE and ESS trend, the conventional electric grid, has been given high priority in most infrastructures. The main cause of the DER employment importance rising and ESS is the increasing need for a decarbonized energy zone in the near future [24].

5.3.1 Internet of Energy

The Internet of Energy (IoE) is defined as the IoT development into distributed energy systems containing SG elements, including distributed sources, data warehouse systems, smart meters, and equipment, such as circuit breakers, digital relays, and transformers [25]. It initiates the inner-connection and peer-to-peer (P2P) transaction of energy and continues it. The most significant aim of IoE is to gather and summon data from distinctive grid edge elements throughout the accessible framework to all other grid control contributors clearly and promptly.

5.3.2 Modern methods for computation

According to computational techniques growth, especially in data analytics, some trending ML and DL methods have been applied in various applications and businesses. The DL is being used for feature engineering and big data management (especially when it is real-time) where ML methods fail. DL also contains large advanced neural networks consisting of several layers, including processing units,

activation functions, and enhancing training methods to learn functional patterns from a great dataset.

In the SG applications, according to current and combined new technologies assembled together for the ESN monitoring in a more accurate way, approved data analytics and business intelligence methods are applied. There has been appropriate usage of traditional and basic data mining tools in the industries until now. Their goal has been to achieve better results in the field of exact electricity demand estimation. These tools have also been applied for other goals such as energy creation forecasting patterns according to peer behavior in the ESN [26].

Among the mentioned methods in Fig. 5.3, the two methods, convolutional neural network (CNN) and recurrent neural network (RNN), are frequently applied in SGs' applications. For the GIS distribution data analysis and interpretation, the CNN method is suitable. Moreover, RNN is good for handling the sequential and time-series data efficiently. According to Fig. 5.4, which is showing the DL schematic in the SG application, considering SG as massive data analytics, load prediction, and load equalizing circumstances application, it would be useful and effective to employ DL algorithms with the goal of achieving more accurate results.

Discussing about IoT and the IoE, the IoT gateways are emerging the "data gathering, dispatch, and analysis" SGs' networks. For example, an IoT gateway device triggers the dataset to be routed across the IoT network with a two-way interaction structure (i.e., device-to-gateway and gateway-to-cloud).

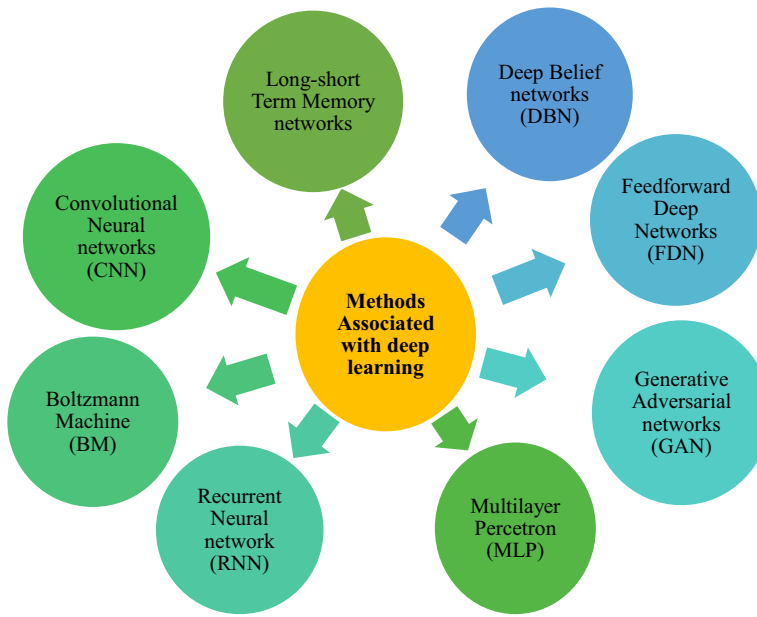


Figure 5.3 Applied deep learning methods.

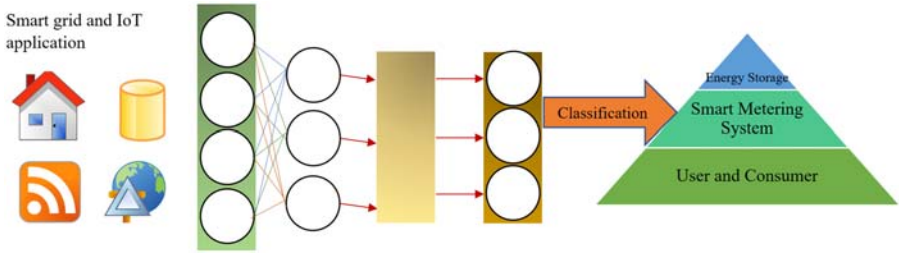


Figure 5.4 A deep learning schema for energy control and management use cases in SGs. *SGs*, Smart grids.

5.4 Internet of Things challenges in energy systems

Improving the electricity power networks needs allowing IoT to access that brings up some issues. Besides database and power sources, the IoT network must be addressed from the electricity business perspective. The reason is that IoT technologies create commercial chances in the electricity industry; however, it poses a risk in the implementation and control process, such as authenticity, surveillance, and identification process. These challenges are being discussed among experts as an important bottleneck in the irregular and ever-changing IoT regions.

In SGs' IoT, considering heterogeneous networks and systems, the network should give prominence to the resilience to support all data types, according to their service quality demands. Different IoT devices generate datasets without complying with any standard, so the data are often depicted in different compositions and configurations [27].

Reference architecture is one of the solutions to address these challenges that play a vital role in the building block representation. These architectures are defined as abstract architectures combined with knowledge and practice in a specific range of application domains. In fact, this incorporation contains development facilitating, order, interoperability, and software systems evolution. Another topic is developing solutions adaptability, which is able to be retained by reorganizing and innovating in design-based solutions conforming to reference architecture. Among the most used and reputable solutions, the trending open IoT platform is considered as a pioneer by being the reference architecture and IoT merger. This platform is designed by guidelines presentation and explanations of detailed automation with regard to required software and hardware [28].

In continue, all challenges categorized by their application are discussed with respect to SGs' experiences all around the world.

5.4.1 Internet of Things attacks

The security challenges and problems encircling the IoT, take place as a threat emerging consequence due to invalid entrances. Critical data flow in the IoT

architecture (i.e., clinical health data, GIS data) and not efficient communication routes facilitate the interconnection of sensors/equipment through a wide range of protocols and standards [29].

Most of the IoT attacks are in the field of proof of concepts weaponization which exploits with destructive charges against popular weaknesses. Many vulnerabilities are left unknown because of differences in IoT systems performance or cost-benefit analysis challenges. As a matter of fact, the proper security controls on IoT devices are an expensive process but demand limited energy resources.

The most threatening IoT attacks are categorized in the following subsets:

- Malware: A destructive software hijacking the sensors' functionality of sensors and expanding in the IoT base. Its target is to gain operational intelligence, which can influence critical equipment connected to IoT devices such as smart meters to be exploited. With IoT devices integration in the SG, many malwares have the ability to damage both the clients and the grid supplier.
- Botnet: An infected device network that spreads across the world. It is controlled in the remote state by a master following the client-server framework.

In the conclusion of reviewing these attacks, there are other issues that come up with the Narrowband 5G approval and the IoT devices topology. A brief review of issues and IoT attacks are discussed below:

- Physical layer attacks on 5G: With the existence of several issues and attacks of this type, the physical channel is vulnerable, which is the path for the device's interconnection [30].
- Selectively jamming primary and secondary synchronization signal (PSS/SSS): Similar to the LTE standard, the 5G also consists of the PSS and the SSS which can be interrupted by a jammer transmitting fake signals [31].
- Sniffing and spoofing vulnerability of the physical broadcast channel (PBCH): The PBCH is utilized by the system information block messages, which cover information about the power thresholds. The information being carried is transmitting unencrypted, leaving it vulnerable to malicious activities [32].

5.5 Future research potentials

Current IoT systems have many advantages highlighted in previous sections for providing energy-efficient solutions in the energy sector. About IoT deployment in the energy domain, new solutions and trends are required to improve the IoT performance and overcome the associated challenges. In the following, we present the blockchain technology and green-IoT (G-IoT) as two approaches to tackle some of the challenges.

5.5.1 Blockchain for Internet of Things

Considering current IoT systems essentially rely on centralized cloud systems, a large number of IoT devices and machines need to be connected in most IoT applications, which is hard to synchronize. In addition, according to the centralized and

server-client nature of IoT, all connected objects are easy to be hacked and compromised. In looking for a solution for these security concerns and privacy issues for users, blockchain will be a good choice.

Blockchain proposes a decentralized platform with no need for a third party's intervention that requires every IoT node to seek the same goal as others. In the form of a block, verified transactions are stored and linked to the previous ones in a way information can never be erased. Additionally, every single transaction history at every node can be recorded, and everyone has access to them. As a result, any blockchain member becomes aware of any changes in each block instantly. Also, with attention to the distributed nature of blockchain, a great number of IoT devices can be synchronized easily. A secure distributed database is provided by P2P networks, so decentralized and private-by-design IoT can guarantee the privacy in need.

In modern energy grids, processed and streaming data is commonly exchanged without limit within the network. Hence, consumers/operators have direct access to power consumption results data without any third-party presence. By simply trading energy between neighbors, a high level of energy costs can be in centralized grids. Another positive point is considered as an area monitoring statistic, which enables the energy flow to be controlled remotely by the power distribution. In this regard, IoT systems help with the equipment fault diagnosis and maintenance process within the SG by blockchain implementation [33].

Despite beneficial cloud and fog computing platforms, there are three obstacles to efficient blockchain technology employment in an IoT-based SG, including computational supply shortage, insufficient bandwidth, and energy retainment.

5.5.2 Green Internet of Things

IoT devices' energy consumption, particularly in large-scale technology deployment of a large scope, is a vital challenge in the coming years. A great quantity of power is necessary to run all of the connected devices to the Internet. A carbon-free and effective communication internet is required to solve these problems, which caused the G-IoT presence. The vital elements in this field are energy measurement characteristics during the life cycle, such as scheme, generation, deployment, and final exposure.

Different IoT technologies, including RFID tags are applications of the G-IoT cycle. For reducing the number of materials used in each RFID tag, the size of RFID tags should be reduced. Another example is green M2M communications, enabling power transmission adjustment to the least amount by deploying algorithmic and distributed computing techniques and getting help from more efficient communication protocols [34].

These are three practical ways for energy management in G-IoT. The first is to get the wireless sensor network nodes in the rest mode and perform just when it is necessary. Second, signal optimization methods, such as synthesis optimization or cooperative connection, are applicable for the nodes' energy consumption reduction. Third, efficient routing methods, such as clustering approaches or multipath routing methods, provide efficient explanations [35].

The modern sustainable power system introduces a more possible strategy for the future SG market share planning according to IoE modern trends. There are some issues with this process, for example, adaptability, connectivity, and most crucial, IoE functions trustworthy among households and consumers. The newly IoE decentralized concept for SG effective management and monitoring is most likely to become ever-present by 2030. The goal in this regard is the overall SG cost minimization, including the investment cost and the operational cost, due to CO_2 emissions restrictions and the operational limitations, Internet devices, and modern carbon-free facilities, which are inconvenient according to new power consumption patterns. While SG power efficiency increases, demand/supply control platforms improvements, and developed interplatforms matching (matter of software) will become possible [36].

5.6 Conclusion

In the new smart era, large-scale usage of IoT technologies in energy systems distributionally and useful energy consumption need integrated IoT structures. Hence, the socioeconomic-environmental, sociological, and economic energy systems' influences will be minimized by helping the energy grid sector change completely from a centralized and clustered supply chain to a decentralized, smart, and optimized IoT enabled system.

In this chapter, the main achievements are the mentioned challenges and pros versus cons discussions instructing a new approach for IoT technologies in SGs. The proposed structure comes with infrastructure, components, challenges, future structures, and applications.

In addition, the modern IoT-based grid management system's advantages were explained, including energy efficiency increase and RE integration. Distinct IoT system components, such as communication facilities and sensors, with attention to their role in the power grid, were also described. Temperature, speed, infrared, humidity, light, and proximity sensors, alongside computing facilities and information analytics platforms, were investigated in detail. Information analytics and data visualization methods were used for several smart functions in the power grids.

Moreover, some IoT application challenges, including object identification issues, big data systems administration, connectivity challenges, systems subsets coordination, safety and availability, IoT grid power requirements, standardization, and system design, were discussed. Trending solutions such as blockchain and G-IoT were also mentioned for these issues.

References

[1] S. Sofana Reka, T. Dragicevic, Future effectual role of energy delivery. A comprehensive review of Internet of Things and smart grid, Renew. Sustain. Energy Rev

Volume 91 (2018) 90−108. Available from: https://doi.org/10.1016/j.rser.2018.03.089. ISSN 1364-0321.

[2] M. Fouad, R. Mali, A. Lmouatassime, M. Bousmah, Machine learning and IoT for smart grid, Int. Arch. Photogramm. Remote. Sens. Spat. Inf. Sci., XLIV-4/W3 (2020) 233−240. Available from: https://doi.org/10.5194/isprs-archives-XLIV-4-W3-2020-233-2020. 2020.

[3] M.A.M. Sadeeq, S. Zeebaree, "Energy management for Internet of Things via distributed systems", JASTT 2 (02) (2021) 59−71. Available from: https://doi.org/10.38094/jastt20285.

[4] S. Sofana Reka, T. Dragicevic, Future effectual role of energy delivery: a comprehensive review of Internet of Things and smart grid, Renew. Sustain. Energy Rev. 91 (2018) 90−108. Available from: https://doi.org/10.1016/j.rser.2018.03.089. ISSN 1364-0321.

[5] A. Merlinda, R. Valentin, F. David, A. Simone, G. Dale, J. David, M.C. Peter, P. Andrew, Blockchain technology in the energy sector. A systematic review of challenges and opportunities, Renew. Sustain. Energy Rev 100 (2019) 143−174. Available from: https://doi.org/10.1016/j.rser.2018.10.014. ISSN 1364-0321.

[6] N.M. Kumar, A.A. Chand, M. Malvoni, K.A. Prasad, K.A. Mamun, F.R. Islam, et al., Distributed energy resources and the application of AI, IoT, and blockchain in smart grids, Energies 13 (2020) 5739. Available from: https://doi.org/10.3390/en13215739.

[7] C. Clastres, Smart grids: another step towards competition, energy security and climate change objectives, Energy Policy 39 (2011) 5399−5408. 10.1016/j.enpol.2011.05.024.

[8] D. Johnson, J.O. Petinrin, S. Oyelekan. Integration of Distributed Energy Resources in Smart Grid System. in: International Conference of Science, Engineering & Environmental Technology (ICONSEET), Ede, Osun State, Nigeria, 2017.

[9] T. Mavroeidakos, V. Chaldeakis, Threat landscape of next generation IoT-enabled smart grids, in: I. Maglogiannis, L. Iliadis, E. Pimenidis (Eds.), Artificial Intelligence Applications and Innovations. AIAI 2020 IFIP WG 12.5 International Workshops. AIAI 2020. IFIP Advances in Information and Communication Technology, 585, Springer, Cham, 2020. Available from: https://doi.org/10.1007/978-3-030-49190-1_11.

[10] A. Ikpehai, B. Adebisi, K.M. Rabie, Broadband PLC for clustered advanced metering infrastructure (AMI) architecture, Energies 9 (2016) 569. Available from: https://doi.org/10.3390/en9070569.

[11] W. Kramer, S. Chakraborty, B. Kroposki, H. Thomas. Advanced power electronic interfaces for distributed energy systems part 1, Systems and Topologies, 2008 10.2172/926102.

[12] A. Ismail, M.S. Abdel-Majeed, M.Y. Metwly, A.S. Abdel-Khalik, M.S. Hamad, S. Ahmed, et al., Solid-state transformer-based DC power distribution network for shipboard applications, Appl. Sci 12 (2022) 2001. Available from: https://doi.org/10.3390/app12042001.

[13] D. Stanelytė, V. Radziukynas, Analysis of voltage and reactive power algorithms in low voltage networks, Energies 15 (2022) 1843. Available from: https://doi.org/10.3390/en15051843.

[14] A.C. Devin, H.K.T.M. Udayanga, L.J. Rohan, BESS as a UPS to power systems with high solar penetration, Front. Energy Res. 9 (2021). https://www.frontiersin.org/article/10.3389/fenrg.2021.653015, DOI = 10.3389/fenrg.2021.653015.

[15] I. Santiago, J. García-Quintero, G. Mengibar-Ariza, D. Trillo-Montero, R.J. Real-Calvo, M. Gonzalez-Redondo, Analysis of some power quality parameters at the points

of common coupling of photovoltaic plants based on data measured by inverters, Appl. Sci 12 (2022) 1138. Available from: https://doi.org/10.3390/app12031138.

[16] Z. Zhu, S. Lambotharan, W.H. Chin, Z. Fan, Overview of demand management in smart grid and enabling wireless communication technologies, Wireless Communications, IEEE, 19, 2012, pp. 48–56. 10.1109/MWC.2012.6231159.

[17] R. Rashed Mohassel, A. Fung, F. Mohammadi, K. Raahemifar, A survey on advanced metering infrastructure, Int. J. Electr. Power & Energy Syst 63 (2014) 473–484. 10.1016/j.ijepes.2014.06.025.

[18] C. Ma, Smart city and cyber-security; technologies used, leading challenges and future recommendations, Energy Rep. 7 (2021) 7999–8012. Available from: https://doi.org/10.1016/j.egyr.2021.08.124. ISSN 2352-4847.

[19] G. Barai, S. Krishnan, B. Venkatesh. Smart metering and functionalities of smart meters in smart grid: a review, in: 2015 IEEE Electrical Power and Energy Conference (EPEC), 2015, pp. 138–145. 10.1109/EPEC.2015.7379940.

[20] D. Porcu, S. Castro, B. Otura, P. Encinar, I. Chochliouros, I. Ciornei, et al., Demonstration of 5G solutions for smart energy grids of the future: a perspective of the Smart5Grid Project, Energies 15 (2022) 839. Available from: https://doi.org/10.3390/en15030839.

[21] J. Oyekale, M. Petrollese, V. Tola, G. Cau, Impacts of renewable energy resources on effectiveness of grid-integrated systems: succinct review of current challenges and potential solution strategies, Energies 13 (2020) 4856. Available from: https://doi.org/10.3390/en13184856.

[22] F.E. Abrahamsen, Y. Ai, M. Cheffena, Communication technologies for smart grid: a comprehensive survey, Sensors 21 (2021) 8087. Available from: https://doi.org/10.3390/s21238087.

[23] X. Wu, T. Kerekes, Flexible active power control for PV-ESS systems: a review, Energies 14 (2021) 7388. Available from: https://doi.org/10.3390/en14217388.

[24] A. Sharifi, Y. Yamagata, Principles and criteria for assessing urban energy resilience: a literature review, Renew. Sustain. Energy Rev. 60 (2016) 1654–1677. Available from: https://doi.org/10.1016/j.rser.2016.03.028. ISSN 1364-0321.

[25] P.K. Khatua, V.K. Ramachandaramurthy, P. Kasinathan, et al., Application and assessment of Internet of Things toward the sustainability of energy systems: challenges and issues, Sustain. Cities Soc. 53 (2020) 101957. Available from: https://doi.org/10.1016/j.scs.2019.101957. ISSN 2210-6707.

[26] W. Donglei, G. Minwei, Application of data mining in traditional benchmark evaluation model for buildings energy consumption, Sci. Program vol (2021). Available from: https://doi.org/10.1155/2021/8610050. Article ID 8610050, 13 pages, 2021.

[27] J.J. Moreno Escobar, O. Morales Matamoros, R. Tejeida Padilla, I. Lina Reyes, H. Quintana Espinosa, A comprehensive review on smart grids: challenges and opportunities, Sensors 21 (2021) 6978. Available from: https://doi.org/10.3390/s21216978.

[28] R. Cloutier, G. Muller, D. Verma, R. Nilchiani, E. Hole, M. Bone, The concept of reference architectures, Syst. Eng 13 (2009) 14–27. 10.1002/sys.20129.

[29] I. Butun, P. Österberg, H. Song, Security of the Internet of Things: vulnerabilities, attacks, and countermeasures, IEEE Commun. Surv. & Tutor. 22 (1) (2020) 616–644. Available from: https://doi.org/10.1109/COMST.2019.2953364. Firstquarter.

[30] H.A. Kholidy, Multi-layer attack graph analysis in the 5G edge network using a dynamic hexagonal fuzzy method, Sensors 22 (2022) 9. Available from: https://doi.org/10.3390/s22010009.

[31] A. El-Keyi, O. Ureten, T. Yensen, LTE for public safety networks: synchronization in the presence of jamming, IEEE Access (2017). Available from: https://doi.org/10.1109/ACCESS.2017.2751964.

[32] M. Lichtman, R. Piqueras Jover, M. Labib, R. Rao, V. Marojevic, J. Reed, LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation, IEEE Commun. Mag 54 (2016) 54–61. Available from: https://doi.org/10.1109/MCOM.2016.7452266.

[33] A. Immonen, J. Kiljander, M. Aro, Consumer viewpoint on a new kind of energy market, Electr. Power Syst. Res 180 (2020) 0378–107796. Available from: https://doi.org/10.1016/j.epsr.2019.106153. 106153, ISSN.

[34] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, F. Muralter, A review of IoT sensing applications and challenges using RFID and wireless sensor networks, Sens. (Basel) 20 (9) (2020) 2495. Available from: https://doi.org/10.3390/s20092495. Published 2020 Apr 28.

[35] E. Mohamed, S.M. Elsherif, M. Elsayed Wahed, An enhancement approach for reducing the energy consumption in wireless sensor networks, J. King Saud. Univ. Computer Inf. Sci 30 (2) (2018) 259–267. Available from: https://doi.org/10.1016/j.jksuci.2017.04.002. ISSN 1319-1578.

[36] W. Strielkowski, D. Streimikiene, A. Fomina, E. Semenova, Internet of Energy (IoE) and high-renewables electricity system market design, Energies 12 (2019) 4790. Available from: https://doi.org/10.3390/en12244790.

Data science leverage and big data analysis for Internet of Things energy systems

6

Arman Behnam[1], *Sasan Azad*[2,3], *Mohammadreza Daneshvar*[4], *Amjad Anvari-Moghaddam*[5] *and Mousa Marzband*[6,7]

[1]Department of Computer Science, Illinois Institute of Technology, Chicago, United States, [2]Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran, [3]Electrical Networks Research Institute, Shahid Beheshti University, Tehran, Iran, [4]Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran, [5]Department of Energy (AAU Energy), Aalborg University, Aalborg, Denmark, [6]Electrical Power and Control Systems Research Group, Northumbria University, Newcastle upon Tyne, United Kingdom, [7]Center of Research Excellence in Renewable Energy and Power Systems, King Abdulaziz University, Jeddah, Saudi Arabia

Chapter Outline

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00006-9

6.1 Introduction

Smart grids (SGs) are the intelligent version of power grids well unified with connectivity and information infrastructures to make system monitoring, control, and grid management better. The two-way electricity flow and circulation of data in these structures are the most popular original attributes comparing traditional power grids. For conceiving a generic intuition about big data, the literature history, composition, methods, and facilities are needed to be discussed. The foundation of big data comes from the huge dataset processing issues and lacks suitable storage capabilities [1]. The big data evolution stages are categorized from megabyte (MB) to gigabyte (GB) from the 1970s to late 1980s, GB to terabyte (TB) from the late 1980s to late 1990, TB to petabyte (PB) from the late 1990s to 2012, and PB to exabyte announced commonly in 2012 [2]. There are many disputes about the exact and appropriate big data definition in vast approaches, and it sounds that attaining a consensus and institutionalized description has been always hard. Currently, roughly the popular three kinds of descriptions are architectural, attributive, and comparative explanations [3]. In addition, the term Internet of Things (IoT) itself is hard to define, since it produces great constant data quantity, which is related straight to the storage capacity. Big data is a term for massive structured, unstructured, and semistructured data, which has been used for information generation [4].

The sections of this chapter are presented as follows. In the second section, data science (DS) approaches and tools are discussed. In the third section, big data analytics methods are described. In the fourth section, future potential studies are being considered. In the fifth section, the conclusion of the chapter is brought.

6.2 Data science

With a large amount of structured data available in energy systems gathered by devices and sensors, there is a crucial need for new analytics methods for extracting knowledge out of these datasets [5]. In this section, the theoretical and practical structures of DS from SG problems to final products are discussed assisting the data scientists in solving real-world problems. Many keywords in this field, including data analysis, data mining (DM), big data, DS, machine learning (ML), and deep learning (DL), have been used among experts, which are highly correlated and challenging [6]. The "data analysis" is defined as the data processing by empirical or logical tools for knowledge extraction and practical purposes, while the "data analytics" is defined as instruments and processes that help with an in-depth information insight exploration [7]. Also, "data mining" is referred to knowledge discovery from data, data/pattern analysis, data archeology, and data dredging. In this regard, data sources consist of databases, data centers (DCs), big data warehouses, and the internet [8].

The term "big data" contains many more features and challenges, including massive, noisy, and erroneous data records, high dimensional data, heterogeneous

features, and unstructured data types [9]. In energy systems, big data is generated by IoT networks and devices. There are 5Vs, including volume, velocity, variety, veracity, and value, being used to understand and describe big data [10]. For data understanding purposes and granular data analysis, "advanced analytics" is defined as autonomous content analysis enabled by advanced techniques to discover deep insights and make recommendations in a new SG intelligence or analytics form [11]. Hence, the term "machine learning" is known as a branch of artificial intelligence (AI) with the goal of automating analytical model building. In addition, trends recognition and decision-making with minimal human involvement are recognized as ML purposes. The term "deep learning" is a subset in the ML field, inspired by the human brain's system and its operation termed artificial neural network (ANN) [12]. Hence, distinct from clear definitions discussed till now, the term "data science" is a conceptual field that comprises advanced data analytics, DM, ML, DL, modeling, and some other related disciplines such as statistics, optimization, ranking strategies, and useful information extraction and transforms them into SG decisions [13]. DS is introduced as a new interdisciplinary field that synthesizes statistics, information systems, optimization, communication knowledge, management, and hardware/software engineering to study data and its derivatives by employing a data-to-information-to-knowledge procedure [14]. In the following sections, all aspects of the DS comprehension and implementation are discussed.

6.2.1 Understanding data science modeling in smart grids

To understand how DS is able to play a vital role in real-world problems, different data structures should be categorized at first and then DS steps should be determined from SG understanding to final product and computerization. Commonly, data availability is the fundamental issue in data-driven application system building. The data is categorized in four fields: (1) structured—built up on a well-defined data structure following an approved order, that is, first and last names, phone numbers, addresses, credit/debit card information, stock market reports, and location; (2) unstructured—without any predefined format, that is, input data, e-mails, blog posts, text issues, text documents, audio, videos, images, presentations' files, and web pages; (3) semistructured—providing features from both the structured and unstructured data, that is, HTML, XML, JSON files, and NoSQL/MySQL databases; and (4) metadata—representing data as the data representator, that is, the author information, keywords, file type and size, file creation date, last modification date, and time [15]. DS model development, which is briefly explained in continue, helps scholars for data analysis in a discussed problem domain and gain insights out of the data to achieve a data-driven model or a product [16].

6.2.2 Steps of data science modeling in smart grid

DS model development from collected data to data product is shown in Fig. 6.1. In the following, each step of this DS process is concisely explained:

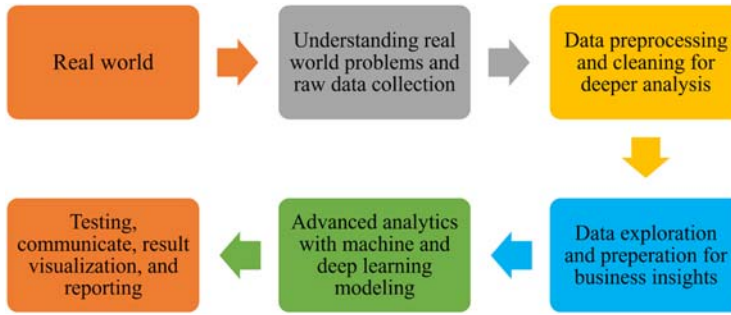


Figure 6.1 Data science modeling from real-world data to the data-driven system and decision-making.

- *The SG domain understanding*: Achieving a complete problem understanding throughout the SG domain is an initial task considering the impacts on the relevant firms/individuals and the ultimate targets. In this regard, there should be questions including which category/group is the target, which action/option should be chosen, etc. These questions depend on the problem's nature and are recommended to be asked at the beginning. These activities are essential to find more information about SG requirements and the expected information from data. This will result in enabling firms to improve their decision-making system, which is recognized as "SG Intelligence" [17]. Another vital step is the data source identification that will help with formulated question answering, also actions and trends based on the data. When the SG problem is defined clearly, the analytical tool or approach is used for the problem-solving.
- *Understanding data*: With a data-driven model/system, fine data understanding is the next step. The data preprocessing tasks are needed to achieve informative insights, which is crucial to any DS employment. Thus data evaluation that assesses the availability of data and its adjustment to the SG problem is known as the data understanding the first job. Several characteristics include data format, the quantity of dataset, quantity sufficiency, relevancy, data authorized access, variable importance, linking several data sources, data evaluation outputs, etc. [18]. They are undoubtedly essential for understanding the data for a discussed SG problem. Generally, the data understanding pipeline helps know the needs of data and the best ways to obtain it.
- *Data preprocessing*: In the beginning, a statistical developed model is needed besides providing tools for hypotheses creation by mostly data visualization and interpretation such as charts, pi-plots, and histograms. The data quality assurance, which is available by the data preprocessing methods, is generally the raw data transformation and cleaning procedure before data analytics. It is also associated with information format manipulating, adjusting data, and combining datasets to refine data. Then, several activities, including missing values imputation and manipulation, unbalanced data and bias problem-solving methods, statistical distribution modeling, dealing with outliers/anomalies, etc., are known as the key elements in this phase [19].
- *Machine learning methods and model evaluation*: Whenever the data is preprocessed for the model building, data scientists are ready to develop a model/algorithm to address the target problem. They are commonly distinct training and test sets of the given data. The division is mostly in the ratio of 80 to 20 or consideration of the most standard k-fold data partition tools [20]. To maximize the model performance, it should be observed every

moment. Several model validation and evaluation metrics, including accuracy, true and false positive/negative rates, precision, recall, F-score, error rate, (receiver operating characteristic curve) ROC, etc., can be used to evaluate the model performance, which helps to choose or design the learning structure [21]. Furthermore, many advanced analytics tools and approaches, including feature engineering/selection/extraction, parameter tuning, ensemble methods, etc., are available for machine learning experts to shape the final data-driven model to deal with a specific SG problem by smart decision-making.

- *Data science product*: Every DS activity output must be a DS product. A DS product generally is a data-enabled product, which is either SG exploration, prediction, data as a service, recommendation engine, data insight, making decisions, classification, clustering, knowledge, paradigm, application, or system. Thus, for decision-making improvement, great distinct machine learning pipelines and DS procedures should be developed [22].

Overall, implementation of DS methods can affect SG practices to alter the performance. The most appealing section in the DS procedure is attaining a further comprehension of the SG problem. If it does not happen, data collecting will be more difficult, which ends in performance decreasing for useful information extraction and decision-making. Talking about the role, "data scientists" usually interpret and study the data to expose the most substantial questions' answers, so organizations'/firms' decision-making procedure will be smoother [23]. In conclusion, a data scientist actively collects and interprets datasets out of many data sources, so a better understanding of the SG performance will be achieved. They also design and develop machine learning methods/algorithms, with attention to multivariational analytics, resulting in intelligent computing.

6.2.3 Advanced data analytics and smart computing in smart grids

Forecasting trends, episodes, and attitudes are cases used for advanced analytics methods and smart computing capabilities. Hence, advanced data analytics is known as automated or semiautomated content analysis to discover more informative insights, prove assumptions/hypotheses, and predict trends and make recommendations where machine learning comes to help [24]. In this regard, key SG questions should be asked, that is, "What is happening?," "Why did it happen?," "What will happen in the future?," and "What operation should be taken?." According to these questions, the data analytics will be divided into four categories, including descriptive, diagnostic, predictive, and prescriptive.

1. *Descriptive analytics*: Finding out the SG changes by historical data interpretation is categorized as descriptive analytics [25]. Thus, to answer the question "what has happened?," historical data summarization has been used. To present a precise SG problem's picture and its relation to previous times, descriptive analytics is important since utilizing a vast range of data is considered in this regard. At last, the definition of strength/weakness points is determined by administrators and managers.
2. *Diagnostic analytics*: The examination of content to answer the question, "Why did it happen?" [25]. Simply finding the problem origins is the goal of this type of analytics. It also enables value extraction from the dataset by suggesting the necessary questions and

deeply interpreting them to attain helpful answers. It is identified by techniques including data distribution interpretation, data visualization, and DM and recognizing the correlations.

3. *Predictive analytics*: It is an essential data analytics method for various purposes and several applications such as SG risk management, power consumption patterns, and predictive and prescriptive maintenance, enhancing their performance [26]. Modern SGs, for instance, simply use predictive analytics for cost minimization purposes by forecasting future demand trends and managing power flow and inventory, production capacity optimization, etc. As a result, predictive analytics is named as the DS analytical core.
4. *Prescriptive analytics*: For the overall rewards and profitability maximization purposes, prescriptive analytics finds the most usage out of available information, so the question "What operation/action should be taken?" can be answered [27]. Prescriptive analytics is known as the last part of the SG analytics, which gathers data from several predictive/descriptive data sources for the application of making decisions. So, its relation with predictive/descriptive analytics is obvious, but the difference is in the priority of actionable insights instead of data monitoring. Integrating ML, DL, SG domain knowledge, big data, and prescriptive analytics aids in the data-driven decision-making process for firms and organizations.

In conclusion, the reasons and the clues of occurrence should be clarified. Hence, descriptive and diagnostic analytics will operate historically. Historical records of data aid in predictive analytics and prescriptive analytics, so the steps that should be taken to make an impact on the discussed analytics will be clear. Forward-looking firms/organizations in the SG practices can use all these analytical methods for smart decision-making. All these results are summarized in Table. 6.1.

6.2.4 Supervised and unsupervised learning in smart grids

There are two learning algorithms that are fundamental categories of ML. While we learn about them early in our DS journey, we might not fully understand their differences, their use, and how we should approach them as engineering problems. Supervised learning is a machine learning method where output vectors and target

Table 6.1 Analytics methods and their description.

Analytical method types	Question answered by the method	Examples
Descriptive analytics	What happened in the past?	Summary of historical events
Diagnostic analytics	Why did it happen?	Anomaly detection and casual relations and effects
Predictive analytics	What is the result in the future?	Grid outputs prediction, recommendation engines, and availability and planning prediction
Prescriptive analytics	What operation should be taken?	SG management improvement

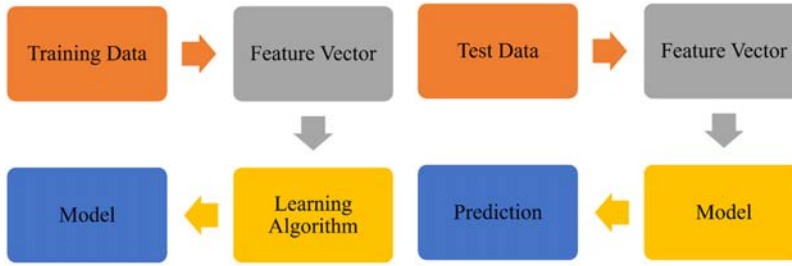


Figure 6.2 Data-driven modeling and training and model testing.

labels correspond to prediction using dataset and features as input [28]. Unsupervised learning is a branch of ML where we apply statistical learning methods to understand our data or create a better representation of it [28]. In this case, we do not have explicit labels.

In Fig. 6.2, a comprehensive ML-based modeling structure discussing the training and testing phase is shown. In continue, several methods, including classification and regression, association rules analytics, time-series analytics, behavioral and log analysis, etc., are explained and illustrated.

6.2.4.1 Classification

Classification is defined as the recognition and grouping process of objects into determined labels. By the precategorized training sets, classification in ML problems leverages many algorithms to classify future test sets into respective and appropriate categories. These classification methods utilize input training datasets aiming at the likelihood or probability prediction [29].

Some classification models are discussed in the following. First, Naive Bayes considers independent predictors, meaning that features are unrelated to each other. Second, the decision tree is used for visual decision-making representation. It is usually made by a yes/no question asking and splitting the answer to move to another decision. Third, k-nearest neighbor (KNN) is used for data division into classes based on the distance between the data points. This method assumes that close data points must be similar and the data points to be classified will be grouped with the closest cluster.

6.2.4.2 Regression

It is a supervised learning method to find the correlation between variables helping scientists with the continuous output variable prediction based on the independent variables. Regression's most popular use cases are forecasting, time-series modeling, and determination of the cause−effect relationship between variables. Simply, regression represents a curve (or a line) passing through all the data points on the target variable graph in such a way that the vertical distance between the data

points and the regression line is minimum. The distance between data points and curves interprets the strength of the model [29].

Some regression models are discussed in the following. First is a linear regression, which shows the linear relationship between the independent variable (X-axis) and the dependent variable (Y-axis). The second is a polynomial regression, in which the original features are transformed into polynomial features of a given degree and then modeled using a linear model. The third is a support vector regression (SVR), which tries to determine a hyperplane with a maximum margin so that the maximum number of data points is covered in that margin. The SVR's main goal is to consider the maximum data points within the boundary lines and the hyperplane.

6.2.4.3 Clustering

It is a method in the field of unsupervised ML, which is known in many DS areas for statistical data analytics. Clustering algorithms are usually for the structure's recognition within a dataset. In the case of a lack of knowledge about groups and categories in the dataset, it will help with the classification of homogeneous groups of cases. In other words, identical data records are in a distinct cluster, which is different from other records in another cluster. Hence, various records sorting into homogeneous internally and heterogeneous externally groups are the most popular clustering goals. It even gives data scientists insight into how data is distributed in a given dataset or as a preprocessing phase for other algorithms.

Through the literature, K-means, hierarchical clustering, and CLARA are categorized into partitioning methods. Also, Density-Based Spatial Clustering of Applications with Noise and ordering points to identify the clustering structure (OPTICS) are categorized into density-based methods. The single and complete linkages are tools for implementing hierarchical methods. There are several categories left in this field: SG-based clustering algorithms, including STING, CLIQUE; model-based clustering such as neural networks, Gaussian mixture model, self-organizing map; and constrained-based algorithms including COP K-means, cyan, magenta, yellow, key (CMWK)-means, etc. [30].

6.2.4.4 Association rules learning

It is recognized as a rule-based learning system in the unsupervised learning area, which is mostly used for a relationship between features' establishment. Association rules learning is a descriptive method often used for large dataset analysis with the goal of pattern discovery. Its essential strength is its completeness and comprehensiveness, which is viable via user-operational constraints such as minimum support and confidence value.

It also helps a scientist to find and interpret trends and cooccurrences within large datasets. In an SG, for instance, the organization infers knowledge about the behavior of devices in terms of power, data flow in the system, etc. that will smooth the production plan change. Most known association rules methods are frequent

pattern-based, logic-based, tree-based, fuzzy rules, etc. In addition, the rule learning algorithms including AIS, Apriori, Apriori-TID, and Apriori-Hybrid, FP-Tree, Eclat, and RARM enable SGs for appropriate problem-solving. Apriori is the most popular implemented method for association rules discovery from a given dataset between all association rules learning methods [31].

6.2.4.5 Prediction and analytics for time-series data

When a dataset is indexed by the date and time stamp specifically including date and time stamp, it is called a time-series data type. From the frequency perspective, the time series are categorized into distinct types, including annual budget and expenses, monthly expenditure computation, and power and energy metrics (daily).

Mathematical modeling for time-series data and fitting process is known as time-series analysis. There are several popular time-series prediction algorithms being used for useful information extraction applications. For example, for time-series forecasting applications with attention to time patterns, the autoregressive (AR) model learns the behavioral trends or patterns of the historical data. Another algorithm is moving average (MA), which is a form of time-series smoothing and forecasting using historical errors in a regression model to interpret averaged trends [32].

The autoregressive moving average (ARMA) combines these two last methods, where AR extracts the momentum and pattern of the trend, and the MA captures the noise effects. The autoregressive integrated moving average (ARIMA) model is an extension of ARMA, which is a frequently used time-series model. As a generalization of an ARMA model, ARIMA is more adaptive than other statistical methods, that is, exponential smoothing and linear regression. The ARMA model is only available for stationary time series, even though the ARIMA model is usually being used for cases of nonstationarity as well. Likewise, seasonal autoregressive integrated moving average, autoregressive fractionally integrated moving average, and autoregressive moving average model with exogenous inputs model (ARMAX model) are other algorithms for time-series data [33]. Furthermore, ML-based and DL-based approaches are appropriate for effective time-series analytics, which is typically used for SG's power flow and consumption, manufacturing, event data, IoT devices data, and commonly in any applied science and engineering temporal measurement domain in SGs. All these time-series-based data analytics algorithms are shown in Fig. 6.3.

6.2.4.6 Behavioral data analysis

Behavioral data analysis helps with revealing new insights into SG sites and IoT applications, power flow behavior, and operators' behavior. It helps in pattern understanding and identifying the reason behind them enabling more accurate activities. Cohort analysis is a division of behavioral analytics that concentrates on studying behavior changes over time. Its popular methods are behavioral data clustering, behavioral decision tree classification, behavioral association rules, etc. [34].

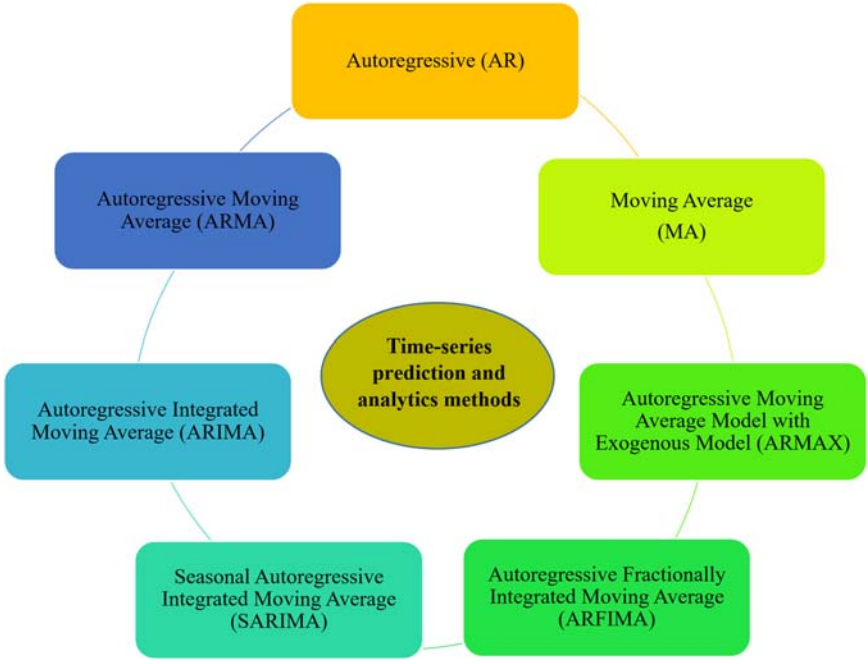


Figure 6.3 Time-series data prediction and analytics methods.

6.2.4.7 Anomaly detection

This section of AI is also known as outlier analysis, which is a DM phase detecting data points, and events that deviate from the regularities or normal behavior of a dataset. Anomalies are commonly recognized as outliers, noise, abnormalities, novelties, inconsistency, and exceptions. Exploring new situations and cases is viable via anomaly detection methods deviant based on historical data by interpreting data patterns using historical data.

Different data sources such as logs, facilities, the internet, and servers generate data that can be used in case of inconsistency removal in anomaly detection. While supervised learning, many ML algorithms including KNN, isolation forests, and clustering ease the anomaly exclusion process that results in a statistically substantial accuracy growth [35]. Nevertheless, extraction of useful variables, recognition of normal trends, imbalanced data management, addressing variations in abnormal behavior or irregularities, sparsity of abnormal events, circumstantial variations, etc. are challenging in the anomaly detection procedure. Anomaly detection applications are cyber-security analysis, intrusion, fraud, fault detection, and also ecosystem disturbance detection [36].

6.2.4.8 Factor analysis

Factors are considered as explanation of relationships or correlations between features. So, factor analysis (FA) is a learning method based on fundamental entities.

Its application is mainly feature organization by comparing them according to their total variance, with attention to mathematical and statistical procedures. The goal of FAis to determinethe features (factors) set number by degree calculation, so the fundamental impact underlying the data will be exposed. As a result, it will be clear which factors are associated with each other and also which factors contribute to the target variable. The ultimate purpose of FA is data summarization so that patterns between factors (variables) can easily be interpreted.

The two most common FA techniques are exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). Recognition of complex trends is possible by EFA analyzing the dataset and prediction evaluation. On the other hand, CFA's mission is to validate hypotheses and use path analysis figures for factor representation [37]. FA is categorized in unsupervised learning with the goal of dimensionality minimization. The most popular FA methods are principal components analysis, principal axis factoring, and maximum likelihood [38]. Also, for the quantification of the statistical interpretation between two continuous factors, some correlation analyses, that is, Pearson correlation analysis are being used.

6.2.4.9 Logs analytics

The data that record system runtime activities in detail and production patterns are known as logs. Log analytics is more of an interpretation approach, which is able to understand generated records/messages. Types of logs are system log, event log, device log, server log, network log, audit trail, record, etc. Data logging is defined as record creation. Many programmed technologies, such as network devices/servers and operating systems, generate logs. There are many smartphone devices in SGs that generate call logs, SMS/MMS Logs, app monitoring logs, notification logs, etc. In SGs, operators' actual behavioral activities with their devices are available as the main characteristics [39].

Appropriate log analytics tools are ML models, classification based on tagging, correlation analysis, and pattern recognition algorithms. Within SGs, log analysis helps with compliance with security procedures and power grids' regulations. It also finds the gaps in the system performance and so it supplies a better user experience by triggering the technical issue solving services. For example, log files are being used to record data on the internet between devices and among grid servers [40].

6.2.4.10 Deep learning and artificial neural networks

ANNs are used for building a computational architecture based on specific processing layers, including the input and output layers, and between them, the hidden layers. The most essential advantage of DL in comparison with regular ML methods is the performance from a complexity and time point of view, especially during the time of training on the large datasets. The most effective and popular DL methods are multilayer perceptron, convolutional neural networks (CNNs), and long short-term memory (LSTM) networks [41]. There is also the "backpropagation"

technique, which adjusts the weights internally in the model structure building process. CNNs are developed on the basis of ANNs, consisting of convolutional layers, pooling layers with filters, and fully connected layers. Its use cases are natural language processing, speech enhancement and recognition, image processing, and autocorrelated data since the two-dimensional (2D) data type is the input of these cases. Advance CNN-based algorithms are AlexNet, Image-Net, Inceptions, Visual Geometry Groups (VGG), ResNet, etc. [42].

Furthermore, recurrent neural networks (RNNs) are another popular kind of DL network and some algorithms such as LSTM and GRU are categorized as RNN methods. Despite regular feed-forward neural networks, LSTM involves feedback through the network by the connections between units. Hence, LSTM networks are appropriate for sequential data analysis and interpretation, including tasks such as classification, sorting, and prediction for time-series data [43]. Thus, with the sequential data type, RNNs can be widely used.

6.3 Big data

A great amount of data created from different data sources in SGs are named "big data." Big data is mostly for managing and facilitating smart infrastructures in modern power systems. The big data issues in SGs are related to different sources such as including phasor measurement unit (PMU) data, power consumption records, advanced metering infrastructure measurements data, and power system smart meter monitoring, maintenance, and management data [44].

Information technology methods are now available in SGs for solving big data issues. Recent surveys have studied some big data challenges in SG systems including the big data role in technology and management in SGs and future issues [45]. Given the recent advancements in smart technologies, it is essential to study and review big data challenges in SGs with attention to SG-oriented viewpoint's theoretical, analytical, and standardized features. In this regard, the research gaps would be the need for the cooperative SG-oriented, information and communication technology−oriented approaches for both scientific communities' experts and public-sector SG administrators and operators as big data application users with limited information of big data challenges. In the following sections, the literature, application, and management approaches for big data are discussed.

6.3.1 Big data in smart grid literature

Based on various definitions of big data, the current big data can be compared to traditional data in order to clarify its applicableness. For the classification of big data characteristics, new methods are needed based on distinct definitions from typical data sources [46]. The dataset records quantity is rising daily by the scale of TBs and PBs because of the emerging big data. Classified structures recommended by big data instead of typical data structures in traditional data sources are

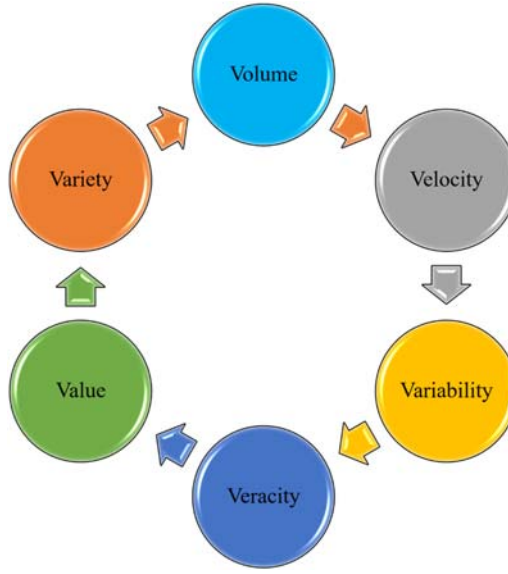


Figure 6.4 Big data 5Vs.

considered as another advantage. The big data velocity characteristic is mainly for computation of the processing rate in the dataset, which is really needed for the data streams and the real-time applications. At last, the goal of big data processing will be extraction of important values from the huge amount of data for real-time applications in SGs.

Volume (dataset size), velocity (the process of collecting big data and analyzing its speed and timeliness), variety (structured, semistructured, and unstructured heterogeneous data types), value (information extracted from big data sparsity), veracity (big data structures credibility and safety), and variability (data attribute modification) are the most essential attributes known as big data 5Vs [47] as shown in Fig. 6.4.

6.3.2 Big data architecture in smart grids

The big data system architecture can be demonstrated as a value chain consisting of four phases that are discussed in the following. While these four phases are defined and are under consideration, the raw data created by big data sources are analyzed and modified for gaining knowledge with attention to distinct management and control goals.

1. *Data generation*: Big data generation along with its types, characteristics, and origins from various data sources is the task of this phase.
2. *Data acquisition*: Aggregates of big data for effective outputs are discussed in this phase, including tasks such as data gathering (information retrieval from sensors and measurement facilities in SGs), preprocessing (errors integration, eliminating redundant records,

and compressing the results), filtering, features engineering, and transmission [transferring data into DCs for storage by communication infrastructures] [48].

3. *Data storage*: Big data storing and management for future applications are tasks for this phase.
4. *Data analysis*: Enhancement of the analytical aspects of the procedure to interpret the collected data by modeling methods for classification and other DS approaches discussed earlier. It is the most important phase in big data for making decisions based on big data knowledge in SGs. Big data analytics are also classified into descriptive, predictive, prognostic, and prescriptive analytics according to the depth of analysis, and their methods are classified into data visualization, and statistical analysis. [49].

6.3.3 Big data technologies in smart grids

The big data technology is utilized for a huge amount of data and the case that typical DS methods or other hybrid ML and DL algorithms are not capable to deal with big data architecture issues discussed earlier, that is, data acquisition and data analysis according to restrictions. Newly, big data technologies have emerged in modern grids, which play a critical role in developing an integrated system to supply efficient operations on data so that timely event detection will happen [50]. Big data tool integration is vital in SG applications. For example, state-of-the-art bidirectional communication and big data management technologies are substantial in SGs, that is, dispatchable energy resources containing electrical loads among themselves and development of distributed energy resources (DERs) [51]. PMU data is applicable in smart distribution grids regarding the demand response for power systems and DERs as practical resources of adaptability. The goal of big data technology could be an analytical framework that applies agent-based modeling for data processing purposes in the SG.

Popular big data technologies in SGs are DM, IoT, cloud computing, software-defined networking, and network function virtualization. DM is defined as pattern recognition by means of computational algorithms with approaches such as estimation, ML, and statistics, which are applicable in SGs [52]. Classification of the devices and other facilities performance variables is an example of DM use case in SGs, according to their power consumption type. Subsequently, AI methods are applicable for designing a risk model and solving uncertainty issues within load forecasting. These methods are developed with the fuzzy wavelet neural network to help in predicting power consumption and also a singular nonparametric estimation algorithm for the power distribution network scheduling [53].

Uncertainty and load-profile volatility, which are measured by smart metering data, are among the issues in SG load forecasting. Heterogeneous big data in the SG causes data-driven decision-making based on data streaming and load-profile behavior prediction with the help of ML and DL methods [54]. These methods are applied for grid energy management, safety, and security purposes. For instance, DL is able to enhance the AI performance through complicated data management, so SG administrators and data scientists are able to extract complex trends automatically, intelligent interaction with devices for maintenance and production, and more precise power load forecasting [55].

6.3.4 Big data tools in smart grids

Here, some of the useful tools for big data analysis, such as Apache Drill, Hadoop, game theory, and DCs, are discussed.

6.3.4.1 Apache Drill

The end users of SGs give the managers and administrators real-time interaction by computers and processing units helping the data to be generated in a more interactive environment. Apache Drill is mainly a distributed system providing interactive analysis for big data and its aim is to contain responses with low latency to ad hoc queries [56].

6.3.4.2 Hadoop

Hadoop is the most widespread big data technology applied in SGs, which provides network searching, click-stream analytics, and spam data filtering. The CloudView, which is a framework based on Hadoop, is for local load utilization, management of various architectures, and clusters of big data analysis purposes. Hadoop consists of two essential counterparts: first, Hadoop distributed file system for storing data according to the capacity prioritized by available tasks and second, the Hadoop execution engine for data processing purposes [57].

6.3.4.3 Game Theory

Game theory is a mathematical method for users' behavior analysis in many applications. In the literature, the multistage Stackelberg game is mentioned as an efficient tool for optimization problem-solving in the field of micro-SG energy management. Other AI complicated models including reinforcement learning, dynamic programming, and game theory are applicable in SG's security awareness management [58]. It works as a security-aware resource allocation model in a matching-coalition game scope.

6.3.4.4 Data centers

These tools represent platforms for dense storage of data enabling the system for multiple functionalities such as data acquisition, transmission, and processing. DCs are able to handle big data by maintaining requirements under time restrictions. The characteristics of DCs, including protection, extensibility, redundancy, energy effectiveness, and consistency, can maintain standardized functionality of big data features by an authorized infrastructure [59]. Cloud-based DCs are capable of power efficiency improvement and reduction in the cost of energy. According to the obvious rise in the data generation rate in power grids lately, it is expected that the big data challenges in DCs attract more scholars to pay attention to the potential topics in this regard, which may help to provide better insights for decision-making out of big data in DCs [60].

6.3.5 Big data applications in smart grids

The SG challenges are usually about data generation, preprocessing, distribution, end users, resources, devices, networks, and interaction with one another for applications and purposes. In this part, the big data systems' most important applications in SGs are discussed and summarized. These applications are expanded in distinct power system phases consisting of the power system scheduling, modeling, monitoring, control, security, and safety [61]. Power generation management is an essential application in SGs, which is adaptable for customizing the scheduling and facilitating the decision-making procedure. The great aspects of this application are efficient power load dispatch, the performance of power generation and storage systems, and power grid optimization in terms of production and cost [62].

Another application of big data is renewable energy resources (RERs) and microgrid management, which is a promising technology for forecasting and management improvement. Based on the literature, this technology is applicable to the association of RERs including wind, solar, biomass, and marine energies [63]. Microgrids known as the new integration of distributed power generation methods are considered as another big data application in SGs. In this regard, the most two important tasks are microgrid investment scheduling and microgrid load distribution optimization. Also, demand-side management is another big data technology in smart power systems.

6.4 Future research potentials

In this section, future possible fields of study in DS and big data analysis for IoT energy systems are discussed. First, future challenges should be presented. Herein, SG development needs to bring up and categorize challenges.

6.4.1 Security and privacy

The security issue of SGs is one of the main challenges in the future. In the literature, attacks and defenses on DL models have been detected, which influence models' performance and make the accuracy, credibility, and trustworthiness less. One of a kind of these threats is false data entrance, which enables IoT devices and sensors with different configurations to send false data. This threat causes faulty results, recommendations, and prognosis to the analytics operations.

Also, SGs are dealing with privacy challenges in the context of IoT applications. In this regard, the data that are captured every second in different locations of the grid by the sensors may contain distinct layers of information. This information affects the decision-making process for different senior managers and middle managers. First, sending and receiving sensitive data to servers with different authentications for administrators presents several privacy concerns. The second challenge in the field of privacy will be the loss of data. Third, the SG's database may be exploited by a third party who does not have permission to employ or even access

the information. However, even the current solutions will remain vulnerable and are able to be hacked by robust attacks. In fact, the hacking process is the development of DL algorithm that learns other DL methods' threat detection methods. This process is explained by how these DL methods generate attacks that are difficult to detect.

6.4.2 Internet of Things big data challenges

Due to the great volume of data generated by different IoT devices, several issues are being concerned, including data depository, communication, complexity, and data analysis. The generated data storage for a long time introduces an important challenge because of the lack of ability to be managed using traditional database management tools. Hence, modern specific tools and infrastructures are essential for handling structured and unstructured big data. Furthermore, the IoT big data analytics requires specific technologies for extracting valuable insights including efficient high-tech processors, levelized edge computing tools, and modern, high-quality, and quick software for big data analysis as discussed before, that is, Apache Hadoop.

6.4.3 Deep learning implementation challenges and limitations

Although satisfying results have been achieved by DL models in SGs' data analytics, in some situations these models are not adequate solutions. Several restrictions should be considered; First, a large amount of data is required for providing good results by DL models. Second, the more data is gathered for the database, the more the training process complexity will appear, which is computationally expensive, and extremely time-consuming. Third, limited access to datasets suffers SG transformation scientists since they have to develop specific datasets requiring a great deal of time and effort. Fourth, DL models are not appropriate for similar but not identical purposes. Fifth, in a black-box running process, the model results' accuracy improvement occurs with time, or it may prove a vulnerable point, especially in the prediction process. In black-box models like neural networks, assuring the training performance is difficult and in some situations, the models' results are not effective.

6.4.4 Smart grid data–driven planning, cost management, and quality of service

A SG IoT system construction needs scheduling strategies that must be considered before launching. A development plan must be designed for each section of the grid based on the needs of its devices because avoiding problems and faults including redundant services or uncoordinated power networks will be solved by this planning. Appropriate planning helps with the facilities development and grid services by identifying the required areas and facilitating the legacy systems integration within the new system.

In this regard, the main SG characteristic is the interconnection of the components, which is considered as an expensive service for governments where many devices, sensors, actuators, and software should be deployed. For instance, a smart surveillance system installation needs modern systems and platforms to gather and process data. These prerequisites are expensive to implement and any error often causes high losses. For maintaining a successful SG system, the quality of service (QoS) is an essential characteristic of applications that should be certified. Separate QoS measurements are used for quality examination such as response time, availability, extensibility, and trustworthiness. Many technologies are integrated for SG service development, such as hosting services and storage frameworks. The assurance of QoS provided by the discussed technologies to ensure an adaptable, powerful, and trustworthy energy system is vital.

6.5 Conclusion

Knowledge-based tools such as DS and big data analysis aid us to comprehend the data's nature and use the extracted insight for improving systems' optimization. How to automize the process for working in a more optimized way according to analytics and algorithms used for performance evaluation is important to consider. The data gathering process from energy systems needs to be improved by experienced experts to elevate the performance results. All features that are available by the data gathering should be revised by the DS specialists, so some first empirical studies can help us interpret the data at first and then find the structure to do the related analytics. This analysis will be much different in case of having a large number of transactions (rows) meaning that we are dealing with big data. Some specific distributions and platforms will be used to handle this data and tasks will be scheduled with network and computing-based methods using nodes and connections.

The integration of information and communication in the energy supply chain deploying IoT occurs with a variety range of embedded actuators, devices, and sensors. Although the usage potential of the internet is now appropriate for reaching the energy system devices attaining by standardized communication protocols, IoT in energy system implementation has several challenges, including accessibility, security, controlling the bandwidth, appropriate interface, connectivity, packet loss, and data analyzing. Available and insightful information is being used for the decision-making process in energy systems, which ends in big data according to great data log, namely, vibration, temperature, and flow sensors outputs. All the gathered information will be analyzed in the big data format. The result will be a more accurate prediction, optimized performance, and better fault diagnosis in energy devices.

References

[1] I.A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani, S.U. Khan, The rise of "big data" on cloud computing: review and open research issues, Inf. Syst

47 (2015) 98−115. Available from: https://doi.org/10.1016/j.is.2014.07.006. ISSN 0306-4379.

[2] S. Pradeep, J.S. Kallimani, "A survey on various challenges and aspects in handling big data," in: 2017 International Conference on Electrical, Electron. Communication, Computer, Optim. Tech. (ICEECCOT), 2017, pp. 1−5, https://doi.org/10.1109/ICEECCOT.2017.8284606.

[3] L. Dobrica, E. Niemela, "A survey on software architecture analysis methods," in, IEEE Trans. Softw. Eng 28 (7) (2002) 638−653. Available from: https://doi.org/10.1109/TSE.2002.1019479.

[4] O. Rusu, et al., "Converting unstructured and semi-structured data into knowledge," in: 2013 11th RoEduNet International Conference, 2013, pp. 1−4, https://doi.org/10.1109/RoEduNet.2013.6511736.

[5] K. Zhou, C. Fu, S. Yang, Big data driven smart energy management: from big data to big insights, Renew. Sustain. Energy Rev 56 (2016) 215−225. Available from: https://doi.org/10.1016/j.rser.2015.11.050. ISSN 1364-0321.

[6] I.K. Nti, J.A. Quarcoo, J. Aning, G.K. Fosu, "A mini-review of machine learning in big data analytics: Applications, challenges, prospects," Big Data Min. Analytics 5 (2) (2022) 81−97. Available from: https://doi.org/10.26599/BDMA.2021.9020028.

[7] A. Belhadi, K. Zkik, A. Cherrafi, S.M. Yusof, S. El Fezazi, Understanding big data analytics for manufacturing processes: insights from literature review and multiple case studies, Computers & Ind. Eng 137 (2019) 106099. Available from: https://doi.org/10.1016/j.cie.2019.106099. ISSN 0360-8352.

[8] C. Sarra, Data mining and knowledge discovery. Preliminaries for a critical, examination of the data driven society, Glob. Jurist 20 (1) (2020) 20190016. Available from: https://doi.org/10.1515/gj-2019-0016.

[9] A. Gandomi, M. Haider, Beyond the hype: big data concepts, methods, and analytics, Int. J. Inf. Manag 35 (2) (2015) 137−144. Available from: https://doi.org/10.1016/j.ijinfomgt.2014.10.007. ISSN 0268-4012.

[10] C.L. Stergiou, A.P. Plageras, K.E. Psannis, B.B. Gupta, in: B. Gupta, G. Perez, D. Agrawal, D. Gupta (Eds.), Secure Machine Learning Scenario from Big Data in Cloud Computing via Internet of Things Network, Handbook of Computer Networks and Cyber Security. Springer, Cham, 2020. Available from: https://doi.org/10.1007/978-3-030-22277-2_21.

[11] O. Müller, I. Junglas, J. Brocke, et al., Utilizing big data analytics for information systems research: challenges, promises and guidelines, Eur. J. Inf. Syst 25 (2016) 289−302. Available from: https://doi.org/10.1057/ejis.2016.2.

[12] D.M. Dimiduk, E.A. Holm, S.R. Niezgoda, Perspectives on the impact of machine learning, deep learning, and artificial intelligence on materials, Processes, Struct. Engineering. Integr. Mater. Manuf. Innov 7 (2018) 157−172. Available from: https://doi.org/10.1007/s40192-018-0117-8.

[13] S. Ewa, Modern data science for analytical chemical data − a comprehensive review, Analytica Chim. Acta 1028 (2018) 1−10. Available from: https://doi.org/10.1016/j.aca.2018.05.038. ISSN 0003-2670.

[14] C. Longbing, Data science: a comprehensive overview, ACM Comput. Surv. 50 (3) (2017) 42, Article 43. Available from: https://doi.org/10.1145/3076253.

[15] A. Kumar, S.R. Sangwan, A. Nayyar, Multimedia social big data: mining, in: S. Tanwar, S. Tyagi, N. Kumar (Eds.), Multimedia Big Data Computing for IoT Applications. Intelligent Systems Reference Library, 163, Springer, Singapore, 2020. Available from: https://doi.org/10.1007/978-981-13-8759-3_11.

[16] B.T. Hazen, J.B. Skipper, C.A. Boone, et al., Back in business: operations research in support of big data analytics for operations and supply chain management, Ann. Oper. Res 270 (2018) 201−211. Available from: https://doi.org/10.1007/s10479-016-2226-0.
[17] D. Alahakoon, X. Yu, Smart electricity meter data intelligence for future energy systems: a survey, IEEE Trans. Ind. Inform. 12 (1) (2016) 425−436. Available from: 10.1109/TII.2015.2414355.
[18] Y. Claudia Vitolo, D. Elkhatib, C.J.A. Reusser, W.Buytaert Macleod, Web technologies for environmental Big Data, Environ. Model. & Softw 63 (2015) 185−198. Available from: https://doi.org/10.1016/j.envsoft.2014.10.007. ISSN 1364-8152.
[19] C.-H. Cheng, Y.-F. Kao, H.-P. Lin, A financial statement fraud model based on synthesized attribute selection and a dataset with missing values and imbalanced classes, Appl. Soft Comput 108 (2021) 107487. Available from: https://doi.org/10.1016/j.asoc.2021.107487. ISSN 1568-4946.
[20] F. Steven, Multiple classifier architectures and their application to credit risk assessment, Eur. J. Operational Res 210 (2) (2011) 368−378. Available from: https://doi.org/10.1016/j.ejor.2010.09.029. ISSN 0377-2217.
[21] A.A. Solanke, M.A. Biasiotti, Digital forensics AI: evaluating, standardizing and optimizing digital evidence mining techniques, Künstl. Intell. (2022). Available from: https://doi.org/10.1007/s13218-022-00763-9.
[22] S. Ren, Y. Zhang, T. Sakao, et al., An advanced operation mode with product-service system using lifecycle big data and deep learning, Int. J. Precis. Eng. Manuf.-Green Tech 9 (2022) 287−303. Available from: https://doi.org/10.1007/s40684-021-00354-3.
[23] M. Veale, R. Binns, Fairer machine learning in the real world: mitigating discrimination without collecting sensitive data, Big Data & Soc (2017). Available from: https://doi.org/10.1177/2053951717743530.
[24] M. Marathe, K. Toyama, Semi-automated coding for qualitative research: a user-centered inquiry and initial prototypes. in: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). Association for Computing Machinery, New York, NY, USA, 2018 Paper 348, pp. 1−12. https://doi.org/10.1145/3173574.3173922.
[25] S.G. Heeringa, B.T. West, P.A. Berglund, Applied Survey Data Analysis, 2nd ed., Chapman and Hall/CRC, 2017. Available from: https://doi.org/10.1201/9781315153278.
[26] M. Seyedan, F. Mafakheri, Predictive big data analytics for supply chain demand forecasting: methods, applications, and research opportunities, J. Big Data 7 (2020) 53. Available from: https://doi.org/10.1186/s40537-020-00329-2.
[27] E.T. Bradlow, M. Gangwar, P. Kopalle, S. Voleti, The role of big data and predictive analytics in retailing, J. Retail 93 (1) (2017) 79−95. Available from: https://doi.org/10.1016/j.jretai.2016.12.004. ISSN 0022-4359.
[28] M. Clayton, N. Zoltán, S. Arno, A review of unsupervised statistical learning and visual analytics techniques applied to performance analysis of non-residential buildings, Renew. Sustain. Energy Rev 81 (1) (2018) 1365−1377. Available from: https://doi.org/10.1016/j.rser.2017.05.124. ISSN 1364-0321.
[29] C. Kuster, Y. Rezgui, M. Mourshed, Electrical load forecasting models: a critical systematic review, Sustain. Cities Soc 35 (2017) 257−270. Available from: https://doi.org/10.1016/j.scs.2017.08.009. ISSN 2210-6707.
[30] M.A. Mahdi, K.M. Hosny, I. Elhenawy, Scalable clustering algorithms for big data: a review, IEEE Access 9 (2021) 80015−80027. Available from: https://doi.org/10.1109/ACCESS.2021.3084057.

[31] M. Hahsler, R. Karpienko, Visualizing association rules in hierarchical groups, J. Bus. Econ. 87 (2017) 317−335. Available from: https://doi.org/10.1007/s11573-016-0822-8.
[32] V. Prema, K. Uma Rao, Development of statistical time series models for solar power prediction, Renew. Energy 83 (2015) 100−109. Available from: https://doi.org/10.1016/j.renene.2015.03.038. ISSN 0960-1481.
[33] F. Saâdaoui, H. Rabbouch, A wavelet-based hybrid neural network for short-term electricity prices forecasting, Artif. Intell. Rev 52 (2019) 649−669. Available from: https://doi.org/10.1007/s10462-019-09702-x.
[34] I.H. Sarker, Context-aware rule learning from smartphone data: survey, challenges and future directions, J. Big Data 6 (2019) 95. Available from: https://doi.org/10.1186/s40537-019-0258-4.
[35] G. Padmavathi, D. Shanmugapriya, A. Roshni, "Performance analysis of unsupervised machine learning methods for mobile malware detection," in: 2022 9th International Conference on Computing for Sustainable Global, Dev. (INDIACom), 2022, pp. 201−206, https://doi.org/10.23919/INDIACom54597.2022.9763180.
[36] M. Ahmed, A. Naser, J. Mahmood, Hu, A survey of network anomaly detection techniques, J. Netw. Computer Appl 60 (2016) 19−31. Available from: https://doi.org/10.1016/j.jnca.2015.11.016. ISSN 1084-8045.
[37] N. David Bowman, A.K. Goodboy, Evolving considerations and empirical approaches to construct validity in communication science, Ann. Int. Commun. Assoc 44 (3) (2020) 219−234. Available from: https://doi.org/10.1080/23808985.2020.1792791.
[38] R. Bhatia, S. Benno, J. Esteban, T.V. Lakshman, J. Grogan, Unsupervised machine learning for network-centric anomaly detection in IoT. in: Proceedings of the 3rd ACM CoNEXT Workshop on Big DAta, Machine Learning and Artificial Intelligence for Data Communication Networks (Big-DAMA '19). Association for Computing Machinery, New York, NY, USA, 2019, pp. 42−48. https://doi.org/10.1145/3359992.3366641.
[39] J. Li, H. Li, W. Umer, H. Wang, X. Xing, S. Zhao, et al., Identification and classification of construction equipment operators' mental fatigue using wearable eye-tracking technology, Autom. Constr 109 (2020) 103000. Available from: https://doi.org/10.1016/j.autcon.2019.103000. ISSN 0926-5805.
[40] K. Guo, Y. Lu, H. Gao, R. Cao, Artificial intelligence-based semantic internet of things in a user-centric smart city, Sensors 18 (2018) 1341. Available from: https://doi.org/10.3390/s18051341.
[41] N. Lingling, D. Wang, V.P. Singh, J. Wu, Y. Wang, Y. Tao, J. Zhang, Streamflow and rainfall forecasting by two long short-term memory-based models, J. Hydrol 583 (2020) 124296. Available from: https://doi.org/10.1016/j.jhydrol.2019.124296. ISSN 0022-1694.
[42] N. Wang, Y. Wang, M.J. Er, Review on deep learning techniques for marine object recognition: architectures and algorithms, Control. Eng. Pract 118 (2022) 104458. Available from: https://doi.org/10.1016/j.conengprac.2020.104458. ISSN 0967-0661.
[43] Y. Su, Y. Zhao, C. Niu, R. Liu, W. Sun, D. Pei, Robust anomaly detection for multivariate time series through stochastic recurrent neural network. in: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD '19). Association for Computing Machinery, New York, NY, USA, 2019, pp. 2828−2837. https://doi.org/10.1145/3292500.3330672.
[44] H. Akhavan-Hejazi, H. Mohsenian-Rad, Power systems big data analytics: an assessment of paradigm shift barriers and prospects, Energy Rep 4 (2018) 91−100. Available from: https://doi.org/10.1016/j.egyr.2017.11.002. ISSN 2352-4847.

[45] E. Hossain, I. Khan, F. Un-Noor, S.S. Sikander, M.S.H. Sunny, Application of big data and machine learning in smart grid, and associated security concerns: a review, IEEE Access 7 (2019) 13960−13988. Available from: https://doi.org/10.1109/ACCESS.2019.2894819.

[46] L. Kong, Z. Liu, W. Jianguo, A systematic review of big data-based urban sustainability research: State-of-the-science and future directions, J. Clean. Prod 273 (2020) 123142. Available from: https://doi.org/10.1016/j.jclepro.2020.123142. ISSN 0959−6526.

[47] K. Adnan, R. Akbar, An analytical study of information extraction from unstructured and multidimensional big data, J. Big Data 6 (2019) 91. Available from: https://doi.org/10.1186/s40537-019-0254-8.

[48] T.A. Alghamdi, N. Javaid, A survey of preprocessing methods used for analysis of big data originated from smart grids, IEEE Access 10 (2022) 29149−29171. Available from: https://doi.org/10.1109/ACCESS.2022.3157941.

[49] H.-N. Dai, H. Wang, G. Xu, J. Wan, M. Imran, Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies, Enterp. Inf. Syst 14 (9-10) (2020) 1279−1303. Available from: https://doi.org/10.1080/17517575.2019.1633689.

[50] X. Yu, Y. Xue, Smart grids: a cyber−physical systems perspective, Proc. IEEE 104 (5) (2016) 1058−1070. Available from: https://doi.org/10.1109/JPROC.2015.2503119.

[51] P.D. Diamantoulakis, V.M. Kapinas, G.K. Karagiannidis, Big data analytics for dynamic energy management in smart grids, Big Data Res 2 (3) (2015) 94−101. Available from: https://doi.org/10.1016/j.bdr.2015.03.003. ISSN 2214-5796.

[52] L. Briceno-Mena, M. Nnadili, M. Benton, J. Romagnoli, Data mining and knowledge discovery in chemical processes: effect of alternative processing techniques, Data-Centric Eng 3 (2022) E18. Available from: https://doi.org/10.1017/dce.2022.21.

[53] M. Rafiei, T. Niknam, J. Aghaei, M. Shafie-Khah, J.P.S. Catalão, Probabilistic load forecasting using an improved wavelet neural network trained by generalized extreme learning machine, IEEE Trans. Smart Grid 9 (6) (2018) 6961−6971. Available from: https://doi.org/10.1109/TSG.2018.2807845.

[54] A. Kumari, S. Tanwar, Secure data analytics for smart grid systems in a sustainable smart city: Challenges, solutions, and future directions, Sustain. Computing: Inform. Syst 28 (2020) 100427. Available from: https://doi.org/10.1016/j.suscom.2020.100427. ISSN 2210-5379.

[55] J.M. Górriz, J. Ramírez, A. Ortíz, F.J. Martínez-Murcia, F. Segovia, J. Suckling, et al., Artificial intelligence within the interplay between natural and artificial computation: Advances in data science, trends and applications, Neurocomputing 410 (2020) 237−270. Available from: https://doi.org/10.1016/j.neucom.2020.05.078. ISSN 0925-2312.

[56] L. Ordonez-Ante, T. Vanhove, G. Van Seghbroeck, T. Wauters, F. De Turck, "Interactive querying and data visualization for abuse detection in social network sites," in: 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, pp. 104−109, https://doi.org/10.1109/ICITST.2016.7856676.

[57] S. Ramírez-Gallego, A. Fernández, S. García, M. Chen, F. Herrera, Big data: tutorial and guidelines on information and process fusion for analytics algorithms with MapReduce, Inf. Fusion 42 (2018) 51−61. Available from: https://doi.org/10.1016/j.inffus.2017.10.001. ISSN 1566-2535.

[58] Z. Zhang, D. Zhang, R.C. Qiu, Deep reinforcement learning for power system applications: An overview, CSEE, J. Power Energy Syst. 6 (1) (2020) 213−225. Available from: https://doi.org/10.17775/CSEEJPES.2019.00920.

[59] X. Chu, S. Nazir, K. Wang, Z. Leng, W. Khalil, Big data and its V's with IoT to develop, sustainability, Sci. Program (2021). Available from: https://doi.org/10.1155/2021/3780594. Article ID 3780594, 16 pages, 2021.

[60] S. Talwar, P. Kaur, S.F. Wamba, A. Dhir, Big data in operations and supply chain management: a systematic literature review and future research agenda, Int. J. Prod. Res 59 (11) (2021) 3509−3534. Available from: https://doi.org/10.1080/00207543.2020.1868599.

[61] S.M. Nosratabadi, R.-A. Hooshmand, E. Gholipour, A comprehensive review on microgrid and virtual power plant concepts employed for distributed energy resources scheduling in power systems, Renew. Sustain. Energy Rev 67 (2017) 341−363. Available from: https://doi.org/10.1016/j.rser.2016.09.025. ISSN 1364-0321.

[62] A. Chauhan, R.P. Saini, A review on integrated renewable energy system based power generation for stand-alone applications: configurations, storage options, sizing methodologies and control, Renew. Sustain. Energy Rev 38 (2014) 99−120. Available from: https://doi.org/10.1016/j.rser.2014.05.079. ISSN 1364-0321.

[63] A. Yadav, N. Pal, J. Patra, et al., Strategic planning and challenges to the deployment of renewable energy technologies in the world scenario: its impact on global sustainable development, Env. Dev. Sustain 22 (2020) 297−315. Available from: https://doi.org/10.1007/s10668-018-0202-3.

This page intentionally left blank

Battery cloud with advanced algorithms

7

Xiaojun Li, David Jauernig, Mengzhu Gao and Trevor Jones
Gotion Inc, Fremont, CA, United States

Chapter Outline

7.1 Introduction

Batteries play an essential role in the rapid development of transportation electrification and energy storage systems [1]. Lithium-ion batteries are known for their high energy/power density and low self-discharge. They are becoming more available as the manufacturing cost continues to improve (Table 7.1). Large-scale energy storage systems consist of MWh/GWh batteries that continuously operate under adverse weather conditions. Electric vehicle batteries are subject to road harshness, different driving behavior, and frequent high-current fast charges. These applications call for batteries to become more reliable, safe, and predictable. As such, monitoring and control of Li-ion batteries become more critical. Battery algorithms, such as state of charge (SOC) and state of health (SOH), deliver important information about battery charge and health. This information is critical for maintaining

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00008-2

Table 7.1 Lithium-ion battery for energy storage applications.

Types	Specific energy	Life cycle	Total Installed Cost
NMC	>150 Wh/kg	1200	$410/kWh
LFP	>110 Wh/kg	2000	$359.62/kWh

Note: Cost estimation based on 24hr and 10 MW, without warranty, insurance, and maintenance [2]. *LFP*, Lithium Iron Phosphate; *NMC*, Nickel Manganese Cobalt.

optimal operations of modern energy networks. For example, inaccurate estimation of SOC will force the energy storage battery systems to reduce charge/discharge power or completely shut off, which subsequently affects the grid stability. On the other hand, based on accurate SOH estimation, a modern energy network can reduce the risk of battery failure. In addition, early thermal anomaly detection can foresee thermal runaway, which is catastrophic for energy networks.

As of now, conventional onboard battery management systems (BMSs) are used for monitoring and control. A BMS includes embedded microcontrollers (μC) and peripheral integrated circuitry (IC). Usually, the BMS collects voltage, current, and temperature measurement with dedicated sensing ICs that communicate with a main μC, which then processes the measurements and perform various functions, such as SOX estimation, diagnostics, protection, control, and thermal management. Nevertheless, the microcontrollers are designed to handle simple tasks and have minimal computing power and memory size. It prevents the onboard BMS from executing advanced algorithms. For example, artificial neural networks (ANNs) are becoming popular for SOC estimation [3]. As we will showin this chapter, an onboard BMS might run a trained neural network. However, the ANN must be carefully designed to reduce its CPU and RAM impact. Although the BMS receives numerous data from the measurements of hundreds of cells that it monitors, these data are not stored due to the lack of onboard data storage, making incremental learning impossible for the onboard BMS.

With the further development of Internet of Things (IoT) [4], future BMS is expected to be cloud-connected. As a result, battery data can be seamlessly uploaded and stored in a cloud data platform [5,6], and the power of cloud computing can be leveraged. The cloud computating and data storage can support advanced algorithms to improve battery safety, performance, and economy. There are several significant advantages. Firstly, the cloud database has battery data from not just one pack but numerous Electric Vehicle (EV) Energy Storage System (ESS) battery packs, allowing a massive amount of data to be used for extensive analysis and machine learning (ML) training and validation. Secondly, cloud computing allows complicated algorithms to be executed in real time, such as online ML, which is not possible for onboard μC. Thirdly, the cloud platform allows data collection and feedback from batteries throughout the entire life cycle. These data can benefit other battery processes and applications. For example, battery manufacturing, second life usage, and recycling. As depicted in Fig. 7.1, battery cloud is at the center stage of a successful battery industry.

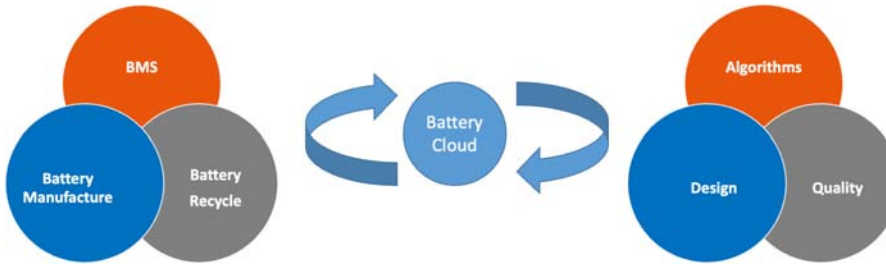


Figure 7.1 Battery cloud is at the center stage of the success of the future battery industry.

This chapter aims to provide an overview of battery cloud, including the essential infrastructure and software components. We also discuss important topics for batteries performance and safety, including the underlying mechanism, effects, and corresponding algorithms. The remaining chapter is organized as follows. The first section discusses the critical components of a battery cloud. In the following sections, we overview the critical areas regarding battery performance, health, and safety: SOC estimation, SOH estimation, and thermal runaway/anomaly detection. This chapter presents corresponding algorithms that were developed with the battery cloud. In the first section, we train and validate an ANN to estimate pack SOC during vehicle charging using remote vehicle data. The ANN is then implemented and tested by onboard BMS. It gives highly accurate ($<3\%$) real-life vehicle testing results. In the second section, high accuracy ($<\%5$) and onboard battery SOH estimation methods for electric vehicles are developed based on the differential voltage (DVA) and incremental capacity analysis (ICA). We extract the charging cycles and calculate the DVA and ICA curves using cloud data. Multiple features are extracted and analyzed to estimate the SOH. At last, a data-driven thermal anomaly detection method is developed for battery safety in the last section. The method can detect unforeseen thermal anomalies at an early stage. In one case, the prediction is more than 1 hour ahead of the event.

7.2 Battery in the cloud

This section covers essential components of a battery cloud. As depicted in Fig. 7.2, it includes the database, data visualization, and algorithm/analytics.

7.2.1 Data sources and connections

Data are collected during different stages of the battery's life cycle, ranging from cell manufacture and module/pack assembly to vehicle driving/charging and pack recycling. There are numerous procedures for cell manufacture alone, including electrode mixing, coating, laser cutting, and stack [7], during which a large amount of data is generated. Table 7.2 shows an example of battery-related data from

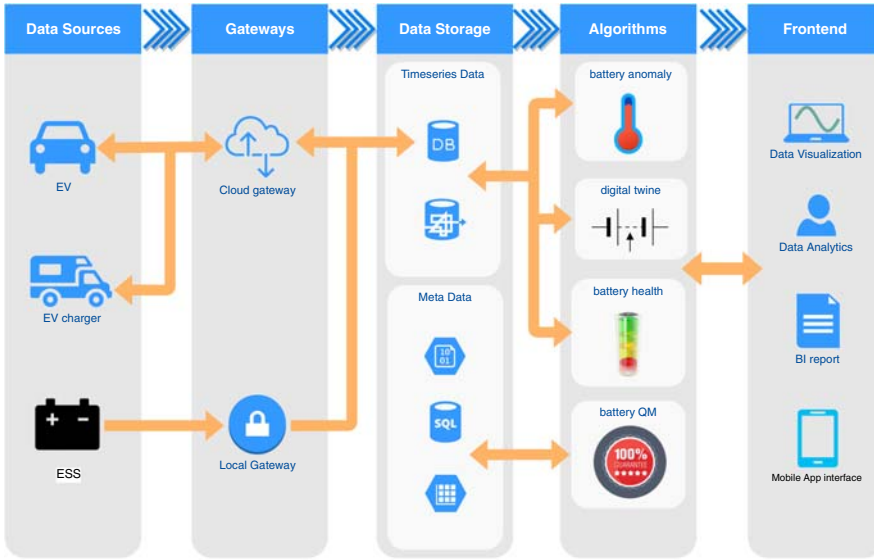


Figure 7.2 Key hardware and software components and data flow of the battery cloud: data storage includes but is not limit to (from top to bottom) NoSQL database, data storage, binary files, SQL database, and spreadsheets.

Table 7.2 Battery data sources.

Item	Stages	Type of data
Cell	manufacture	manufacture metadata battery time series data
Pack	assembly testing recycle	assembly metadata battery time series data recycle metadata
EV&ESS	operation	battery time series data vehicle/grid metadata
Service	service	service event data

different devices and scenarios. The EV battery pack is equipped with a BMS which communicates with a wireless IoT component that transmits the collected data to the cloud via the 4G/5G network. Online or private gateways will be used for charging stations. Because ESS power plants affect grid stability, they are subject to more stringent cybersecurity regulations. As a result, usually, ESSs are connected through a one-way, local gateway to ensure maximum security. Similarly, battery data from cell/pack testing equipment are often transmitted via a secured, one-way gateway. However, these equipments can be controlled securely via the company's intranet.

7.2.2 Database

Choosing the right database. For production big data platforms, Hadoop [8] is the prevailing choice. Hadoop is based on HDFS (Hadoop files system) and MapReduce (the programming model) that ensure good scalability, robustness, and high availability, all of which are essential requirements for a battery database. Besides, Hadoop has a complete ecosystem, including software stacks like Spark, Hbase, Kafka, Hive, and many others, making it easier to use and expand functionalities. There are also dedicated time series databases (TSDBs), such as Influxdb, Timescale, and Prometheus. TSDB has built-in features for time series data, such as time-domain queries (integration, differential). This makes TSDB ideal for a small R&D battery database. As TSDBs are being developed and improved actively, they will become more competitive against traditional databases in the future.

Database deployment. The database can be hosted on-premise or on the cloud. Although on-premise deployment will theoretically give better control and security, it is often more expensive to maintain and scale. For cloud deployment, there are several models to consider. IaaS (Infrastructure as a Service) let the cloud provider handle hardware resources, where the company has complete control of all software stacks. Popular IaaS providers are Amazon Web Services (AWS) [9], Microsoft Azure [10], and Google Cloud Platform [11]. In the PaaS (Platform as a Service) model, such as AWS EMR, the cloud provider also hosts basic software stacks, except for application software. The provider manages all software stacks in the SaaS (Software as a Service) model, such as Cloudera [12] and Influxdata Cloud [13].

7.2.3 Data visualization

Most end-users of battery data are data analysts or operators who monitor EV/ESS in real time. It is vital to have a responsive and interactive data visualization tool where essential data are displayed in real time. Users can create a dashboard and add custom processing/query to explore statistical insights. Other features include (1) adding a signal threshold, which can trigger quick alarms to the ESS site operator, and (2) options to trigger an ML pipeline from the frontend. Many data visualization tools are web-based, such as Grafana, Datadog, and Kibana. Fig. 7.3 depicts an example battery data display dashboard.

7.2.4 Algorithms and analytics

With the data platform built, advanced algorithms that leverage big data and ML [3] can be applied to increase battery performance, safety, and economy. An interesting topic is the digital twin [14]. Based on sophisticated electrochemical modeling, the digital twin can give insight into the internal states of its physical twin, which can be used for battery states estimation, diagnosis and prognosis. The battery cloud platform will need API (application programming interface) for popular programming languages, such as Python and Matlab®, based on the developers' preferences. It may also provide a more interactive development tool such as

Figure 7.3 A typical dashboard for displaying battery data, developed by Gotion [6].

Jupyter Notebook/Lab or Sagemaker, commonly used for data analytics/ML. After the algorithms/analytics are developed, they should be optimized and incorporated into a data processing engine, such as Spark, Kafka, and Airflow. Life data of all the battery cells are used to analyze the manufacture, assembly process, and facility to improve quality management. Similarly, these data can be used as references during battery second life application, recycling, and refurbishing, eliminating the need for extra testing/calibration.

7.3 Onboard state of charge estimation with cloud-trained ANNs

SOC estimation is one of the essential functions of battery software. It has been researched extensively. There are mainly three different methods for SOC estimation. The commonly used, basic method is coulomb counting, which calculates the accumulated charge by current integral, given as

$$z(t) = \frac{1}{C}\int_0^t i(\tau)d\tau + z(0), \tag{7.1}$$

where C is the battery capacity. This method is susceptible to accumulated error generated from $i(t)$ or data loss from $z(0)$. As such, estimation accuracy degrades if coulomb counting is used without correction over a prolonged period of time. The other two methods are model-based and data-driven. Both have self-correction features to correct the SOC. The model-based approach utilizes a battery model, either ECM (equivalent circuit model) or electrochemical model, to establish the

connection between battery measurements, such as voltage, temperature, and current, and immeasurable internal states. Then an estimator, such as Kalman filter, is applied to estimate the SOC. Because those batteries are highly nonlinear systems, modified Kalman filters such as extended Kalman filters and unscented Kalman filters are often used in practice. Model-based approaches require an accurate model. The model can be calibrated accurately by long-term cell and pack testing. But it is also prone to overfitting, meaning it cannot tolerate individual cell/pack variations. Making an accurate and well-generalized model is very challenging and time-consuming. Data-driven approaches range from simple voltage-based correction [15] to deep neural networks [16]. More detailed reviews of data-driven SOC estimation methods are covered by Refs. [3,17]. Most of these methods are resource-consuming and cannot be easily applied to an onboard BMS.

This section presents a data-driven SOC estimation method that fuses the onboard BMS with the battery cloud. A neural network is trained with cloud battery data. Then, it is designed to reduce the computational and memory footprint to be fit into a microcontroller.

7.3.1 Requirements, definition, and design

When designing SOC algorithms, there are typical requirements to be considered. For example:

1. SOC estimation should be 100% when the battery is fully charged.
2. SOC estimation should not change suddenly, including between power cycles.
3. SOC estimation should have a maximum error of less than 5%.
4. SOC estimation should have an average error of less than 3%.

The neural network presented is designed to meet requirements #1, #3, and #4. Other requirements, such as #2, are implemented by a different software component, such as the SOC initialization function.

As depicted in Fig. 7.4, the neural network includes an input layer, hidden layers, and an output layer. The inputs are measurable battery signals, including voltage, current, and temperature. Both present and historical measurements are used. Historical measurements are critical for the feed-forward ANN to infer the internal SOC of the battery, which is a dynamical system.

7.3.2 Artificial neural network training with cloud data

The ANN is developed using Matlab and Simulink®. Cloud battery data are fetched through Matlab API and used to train the neural network. DC charging data of NMC (Nickel Manganese Cobalt) cells are used for training. The training data includes the cells being charged at a range of temperatures, including $-10^{\circ}C$, $0^{\circ}C$, $25^{\circ}C$, $40^{\circ}C$, and $50^{\circ}C$, during which the voltage and current signals are recorded. As depicted in Fig. 7.5, these data are split into training data (75%), validation data (15%), and test data (15%). During the training, Levenberg−Marquardt is configured as the optimization algorithm. The training results are depicted in Fig. 7.6.

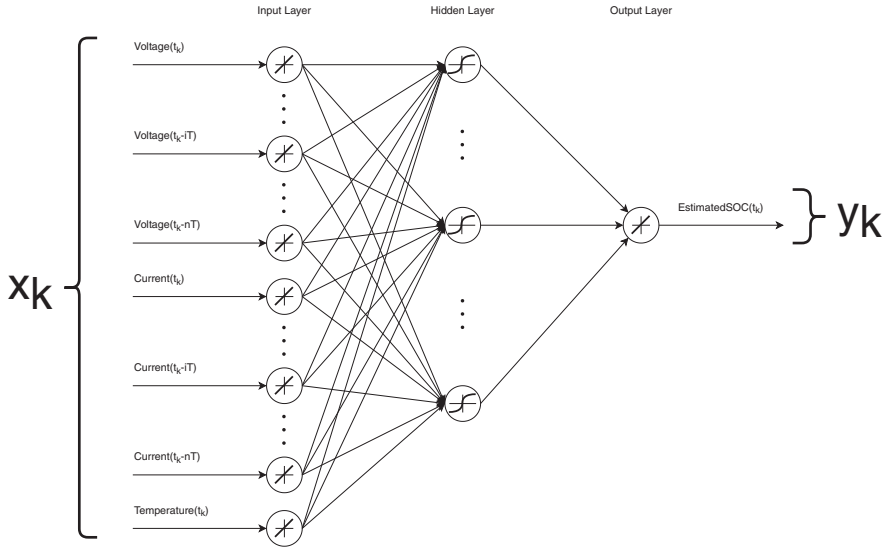


Figure 7.4 The neural network model used for SOC estimation. *SOC*, State of charge.

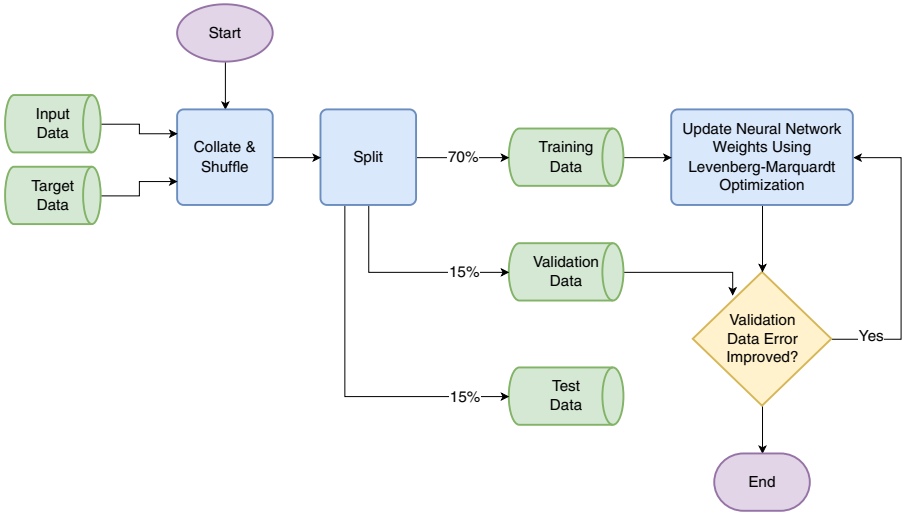


Figure 7.5 The ANN training flowchart for SOC estimation. *ANN*, Artificial neural networks; *SOC*, state of charge.

After acquiring the parameters, the ANN is implemented as Matlab code and integrated into the SOC software component, a Simulink® model. Using the embedded coder, the Simulink® model is converted to C code, integrated with other software components, and eventually become executable binaries.

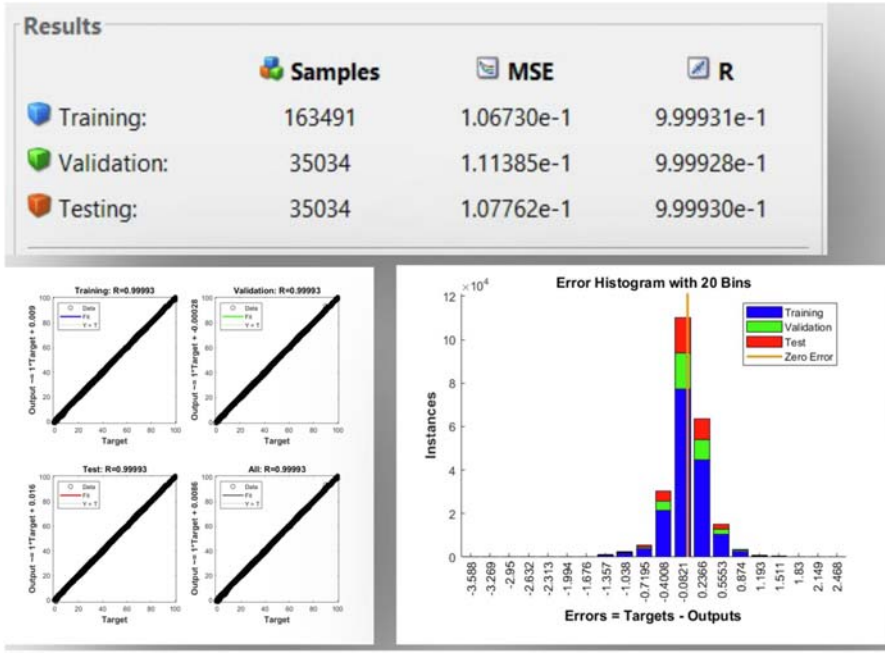


Figure 7.6 ANN training results. *ANN*, Artificial neural networks. Please see the online version to view the color image of the figure.

7.3.3 Hardware-in-the-loop and vehicle testing results

The ANN is first tested using the hardware-in-the-loop (HIL) system, during which basic functions of the software component and SOC accuracy are evaluated using cloud data. More importantly, as the ANN executes in the BMS real-time operating system, the impact on CPU and RAM usage is evaluated. It is found that the ANN takes approximately 50 μs of execution time. Its RAM usage is also small.

Finally, the algorithm is tested on a vehicle BMS. The ANN is deployed as a shadowing strategy in addition to existing software for several passenger EVs. To verify its robustness, the ANN is tested under the AC charge scenario to verify its robustness. Even though it is only trained with DC charge data, the ANN performed satisfactorily during AC charging. For example, Fig. 7.7 depicts the SOC comparison, current, voltage, and temperature plots of one test. As shown in the SOC comparison plot, for most of the time, the true SOC (solid blue) falls into the $+/-5\%$ bracket of the SOC estimation (solid red). The RMSE of all testing results is 1.9%, well below the 3% target.

7.4 Online state-of-health estimation

Li-ion batteries and many other secondary cells are subject to different degradation mechanisms that cause loss of usable energy or power, which lead to a decrease in

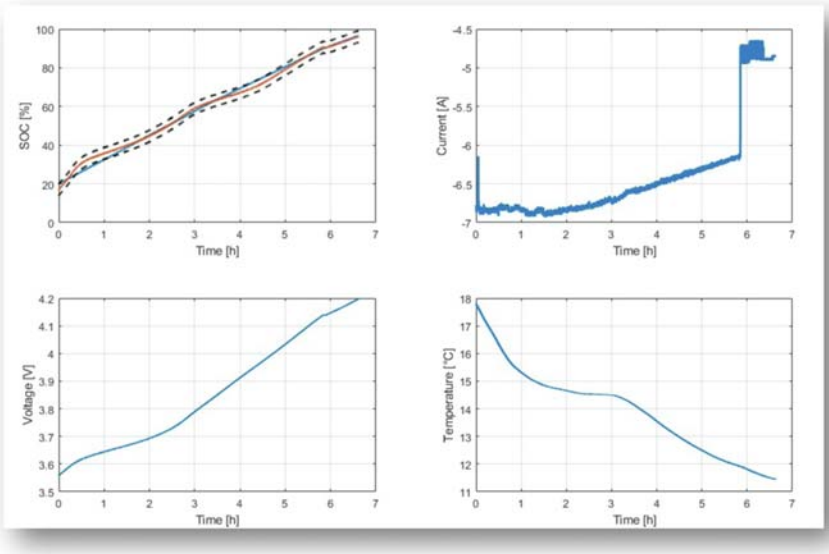


Figure 7.7 Onboard vehicle test: AC charging.

range and acceleration for battery electric vehicle [18]. For that reason, it is essential to monitor the SOH of Li-ion batteries. The degradation mechanisms are briefly discussed and organized into three categories in the following section. Furthermore, the concept of the end of life (EOL) and the SOH_C will be presented. Conclusively, an overview of SOH_C estimation methods will be given, with a closer look at the differential voltage analysis (DVA) and the ICA.

7.4.1 Degradation mechanisms and modes of Li-ion batteries

The components of a Li-ion battery are subject to different degradation mechanisms. In general, the degradation mechanisms can be classified into three modes: [18–20]

- *Loss of lithium inventory* (LLI): The Li-ions are consumed by side reactions and are no longer available for intercalation/deintercalation in the anode and cathode.
- *Loss of active material of the anode* (LAM_A): The anode active material is no longer available for lithium intercalation due to particle cracking and loss of electrical contact or active areas being blocked by solid surface layers.
- *Loss of active material of the cathode* (LAM_C): The cathode active material is no longer available for lithium intercalation due to structural failure, particle cracking, or loss of electrical contact.

These modes can be attributed to different degradation mechanisms in the components of a Li-ion cell. In the following sections, the primary degradation

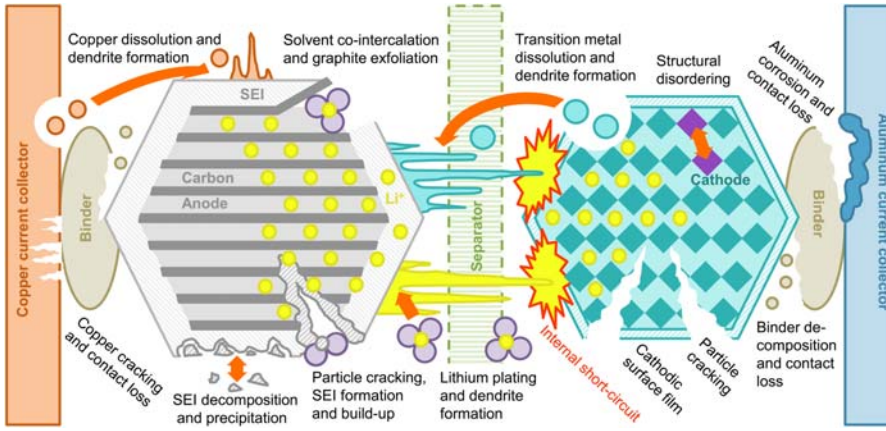


Figure 7.8 Degradation mechanisms in Li-ion cells.
Source: Adapted from C. R. Birkl, M. R. Roberts, E. McTurk, P. G. Bruce, D. A. Howey, Degradation diagnostics for lithium ion cells, J. Power Sources, 341 (2017) 373−386.

mechanisms on the components of a Li-ion cell are named and briefly explained. An overview of these degradation mechanisms is presented in Fig. 7.8.

7.4.1.1 Anode

The main degradation modes at the negative electrode are lithium plating and the formation of solid electrolyte interphase (SEI). Lithium plating is a commonly recognized and inherently damaging degradation mechanism in Li-ion batteries, which describes the deposition of lithium metal on the surface of the anode as soon as the anode potential exceeds the threshold of 0 V (vs Li/Li +) [21]. On the other hand, the SEI is a protective layer on the surface of the anode particles due to the decomposition of the electrolyte, which is formed mainly during the first cycles [22]. Both degradation modes are the main contributor for LLI and LAM_A [18].

7.4.1.2 Cathode

On the other side of the battery, the degradation modes of the cathode are still growing in interest and therefore not thoroughly documented yet. It is considered that structural changes and mechanical stress are the main contributors to LLI and LAM_C. Due to various cathode materials, the Li-ion battery suffers from different side reactions based on the cathode material composition. For example, an Mn-based cathode is more prone to the dissolution of the active material due to Mn dissolution. In contrast, the degradation of the LFP (Lithium Iron Phosphate) cathode is more likely to be defined by Fe dissolution, which generates HF as a byproduct and attacks the surface of the cathode particles [21].

7.4.1.3 Separator, electrolyte, and current collectors

The separator, electrolyte, and current collectors also suffer from various degradation mechanisms. Although the porous separator of a Li-ion cell is electrochemically inactive, the separator can negatively affect the performance of the cell. According to various studies, deposits from the electrolyte decomposition can clog the pores of the separator. This can increase the impedance and also can reduce the accessible active surface of the electrodes (LAM_A and LAM_C, respectively) [19,23].

On the other hand, the electrolyte is involved in side reactions that lead mainly to the formation of a surface film on the negative electrode, but also partly on the positive electrode. Electrolyte oxidation at the cathode does not directly affect any of the three modes of degradation, but it does cause reintercalation into the active material, also known as self-discharge of the cell. In contrast, electrolyte reduction at the anode results in a loss of cyclable lithium, which leads to a capacity loss [24,25]. The current collectors of a Li-ion cell suffer mainly from two degradation mechanism. First, the current collectors can corrode electrochemically. This occurs particularly at the aluminum collector of the positive electrode when acidic species, such as HF, are present [26]. The copper current collector of the negative electrode may dissolve during deep discharge when the anode potential increases to 1.5 V in reference to Li/Li^+ [27]. Second, the current collector foils may deform due to mechanical stress. This can disrupt the contact between the electrodes and the separator so that specific active areas can no longer participate in the intercalation process of Li-ions in to the electrodes, which causes a loss in capacity [28].

Based on Fig. 7.9, it can be seen that all degradation modes can be organized by their effect on the electric characteristics of a Li-ion battery, the capacity and power fade. For further elaborations, we will focus primarily on the capacity fade.

7.4.2 State of health and end of life

Due to the degradation mechanisms, Li-ion batteries have a limited lifetime. The EOL of a Li-ion battery is reached when the battery can no longer provide the power or energy intended for its application [29]. However, as of today, there is no uniform standard that defines a clear EOL criterion for Li-ion batteries in the new energy industry [24]. The USABC consortium is the only one to define two EOL criteria in its manual of test procedures for electric vehicle batteries. According to this manual, the EOL of a Li-ion battery is reached when:

- the net capacity delivered is less than 80% of the rated capacity C_N or
- the peak capacity is less than 80% of the rated capacity at a DOD of 80% [30].

Also, in many publications, the EOL for the Li-ion-based traction battery of a BEV at a capacitive aging condition of $SOH_C \leq 80\%$ assumed [31–33]. The capacitive aging state SOH_C can be calculated using Eq. (7.2). Here, C_N corresponds to the nominal capacity of the Li-ion battery, and $Q_{dis,max}$ corresponds to the

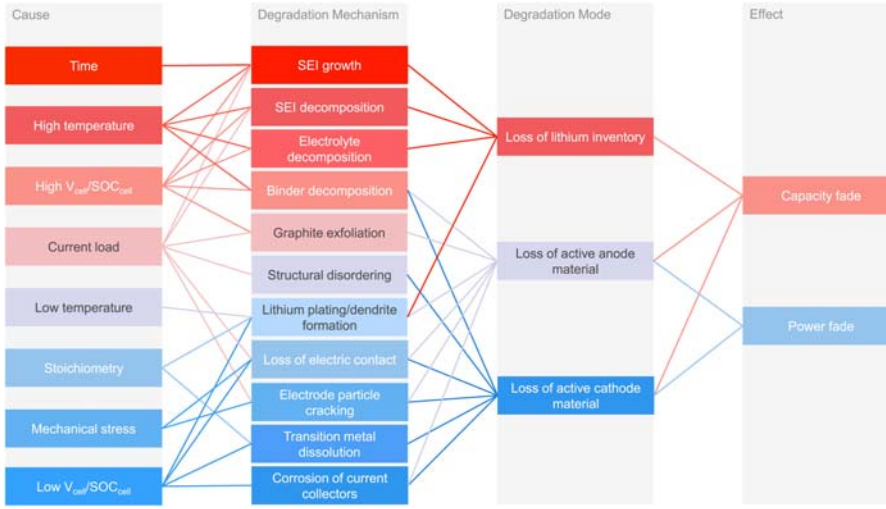


Figure 7.9 Overview of different degradation mechanisms and their cause and effect on the performance of the Li-ion cell.
Source: Adapted from C. R. Birkl, M. R. Roberts, E. McTurk, P. G. Bruce, D. A. Howey, Degradation diagnostics for lithium ion cells, J. Power Sources, 341 (2017) 373−386.

maximum charge quantity that can be removed from a Li-ion battery, which is also known as the net capacity.

$$\mathrm{SOH_C} = \frac{Q_{dis,max}}{C_N} \cdot 100\% \tag{7.2}$$

7.4.3 Advanced online state-of-health estimation methods

The capacitive aging state $\mathrm{SOH_C}$ has an impact on two critical factors of a BEV, the maximum range and the charging time during fast charging. Based on the capacitive aging state $\mathrm{SOH_C}$, the maximum range can be predicted to the driver, and the fast charging function can be adjusted to find the optimal compromise between minimum charging time and damage of the anode by lithium plating [34]. Therefore an online $\mathrm{SOH_C}$ estimation is essential for automotive applications.

7.4.3.1 Methods

There are several options for determining the capacitive aging state, which can first be divided into experimental and model-based methods, respectively. As shown in Fig. 7.10[1], these categories can be subdivided into further subcategories. For example, experimental methods can be divided into direct methods, such as capacity

[1] This figure was published in Journal of Power Sources, 405, R. Xiong, L. Li, J. Tian, Towards a smarter battery management system: a critical review on battery state of health monitoring methods, 18−29, Copyright Elsevier (2018).

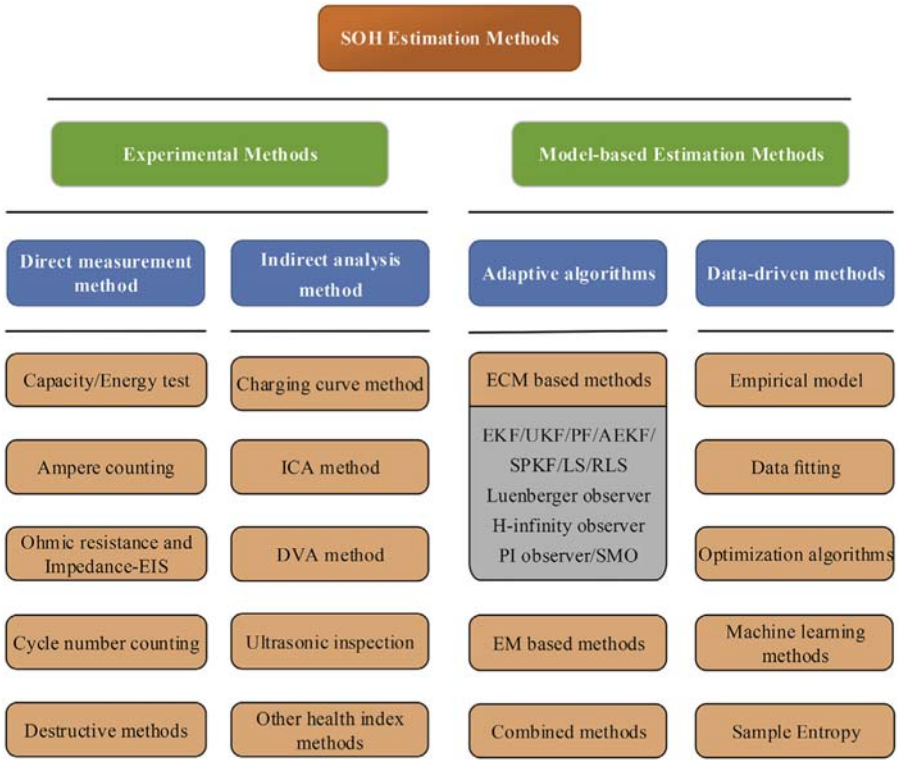


Figure 7.10 Methods for SOH_C estimation.
Source: From R. Xiong, L. Li, J. Tian, Towards a smarter battery management system: a critical review on battery state of health monitoring methods, J. Power Sources, 405 (2018) 18−29.

measurement (coulomb counting), and indirect methods, such as DVA. In contrast, model-based methods can be divided into SOH_C determination based on adaptive battery models or data-driven methods.

At this point, the most popular methods regarding the capacitive aging condition SOH_C are mentioned and briefly discussed. More detailed summaries about methods for SOH_C estimation were given by Berecibar et al. [36]. and Xiong et al. [35].

Direct measurements. These are the most straightforward method to determine the SOH_C. One prevalent method is the direct measurement of the current battery capacity. However, this method requires an enormous expenditure due to the low charging current during the capacity measurement, which is why this method is only used for R&D purposes.

Model-based estimation methods. These utilize algorithms such as Kalman filter or neural networks to model the battery cell parameters. These methods achieve relatively high accuracy and can be implemented in a cloud-BMS. Yet, these algorithms require a high development effort. For example, the accuracy of the Kalman

filter is highly dependent on the accuracy of the applied battery model, whereby high accuracy is only achieved with complex battery models. Also, training a neural network requires a large amount of data, which can only be generated by cost-intensive testing of battery cells. In addition, these algorithms need extensive validation. For example, the neural network is considered a black box, and the output cannot be generally predicted based on unexpected input data.

Indirect analysis methods. These methods utilize various battery parameters to correlate the capacity fade with various features of the Li-ion battery. For example, the charge curve can characterize the SOH_C of the battery as it changes throughout the battery degradation. Constant current followed by constant voltage with current limiting (CCCV) charging mode is commonly used for batteries. Eddahech et al. [37]. developed a method for SOH_C estimation using the CV stage as a health indicator. Since minimal intrinsic information about the battery can be obtained directly from the voltage curves, Dubarry et al. [38,39], for example, used electrochemical characterization and analysis techniques, ICA, and DVA (dV/dQ). These methods are often applied in laboratories since a low current rate is required to record these differential curves. However, due to the increasing energy of the battery packs and the lower power of AC charging, it is also possible to record the differential curves during an AC charging process in a BEV. For this reason, the basics of the DVA and ICA and their correlation with capacity fade will be discussed in more detail in the following section.

7.4.3.2 Differential voltage analysis/ICA-based state-of-health estimation method

As mentioned before, it is essential to estimate the SOH_C of battery packs in BEV. In the following section, a DVA- and ICA-based estimation method is introduced. Therefore the DVA and ICA will be presented and discussed in detail to present a simple SOH estimation implementation, which could be realized on a cloud platform.

The DVA and ICA are commonly known analysis methods for Li-ion batteries in laboratories. The IC curves can be calculated from Eq. (7.3) during a low-current charging or discharging process. The division of an infinitesimal charge change due to the charge/discharge current by the resulting voltage change is calculated. This process converts the low-slope regions of the OCV curve, also known as voltage plateaus of the two-phase transition, into detectable IC peaks. Another method is the DVA (dV/dQ). The DV curves can be calculated by the reciprocal of the IC curve as shown in Eq. (7.4). The distance between two peaks of the DV curve represents the amount of charge involved in the two-phase transition, so it is easier to analyze the capacity degradation quantitatively using the DV curves [40].

$$\frac{dQ}{dV} \approx \frac{Q(t) - Q(t + \Delta t)}{V(t) - V(t + \Delta t)} \tag{7.3}$$

$$\frac{dV}{dQ} = \left(\frac{dQ}{dV}\right)^{-1} \approx \frac{V(t) - V(t + \Delta t)}{Q(t) - Q(t + \Delta t)} \tag{7.4}$$

The result of calculating the IC curve during a low current rate charging process is shown in Fig. 7.11. It should be noted that the DV curves can be represented using the half-cell potentials due to the superposition behavior of the anode and cathode [see Eq. (7.4)]. Thus the peaks and valleys of the DV curve can be assigned to the anode and cathode, respectively.

As mentioned before, Li-ion batteries suffer from various degradation mechanisms, which lead to LLI, LAM_C, and LAM_A. Due to these degradation modes, a change in the DV and IC curves can be observed. Fig. 7.12 shows the shift of the DV and IC curve due to cyclic aging. Based on the change of these features, the SOH_C can be estimated by correlation, for example, the distance between two peaks in the DV curve with the capacity fade of the Li-ion battery. Another possible feature is the height or depth of the peaks or valleys of the IC curve, which also shift throughout the ongoing degradation of battery materials.

In order to implement a DVA/ICA-based SOH estimation on a battery cloud the following workflow should be included:

1. The platform monitors the typical battery cell parameters, voltage, current, and temperature.
2. Whenever the battery is charging, it determines if the charging data has satisfied feature detection based on several conditions. The conditions include the C rates, amount of charge, and so on.
3. If the conditions are met, proceed with the following steps. Otherwise, abort and watch for the next window.

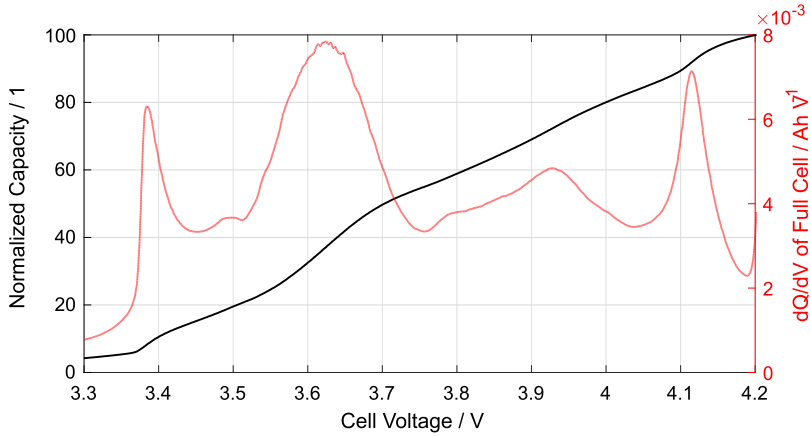


Figure 7.11 The differential curve of ICA during a CC charge with C/10 of a Li-ion battery consisting of a graphite anode and NMC cathode. *CC*, Constant current; *ICA*, incremental capacity analysis; *NMC*, Nickel Manganese Cobalt.

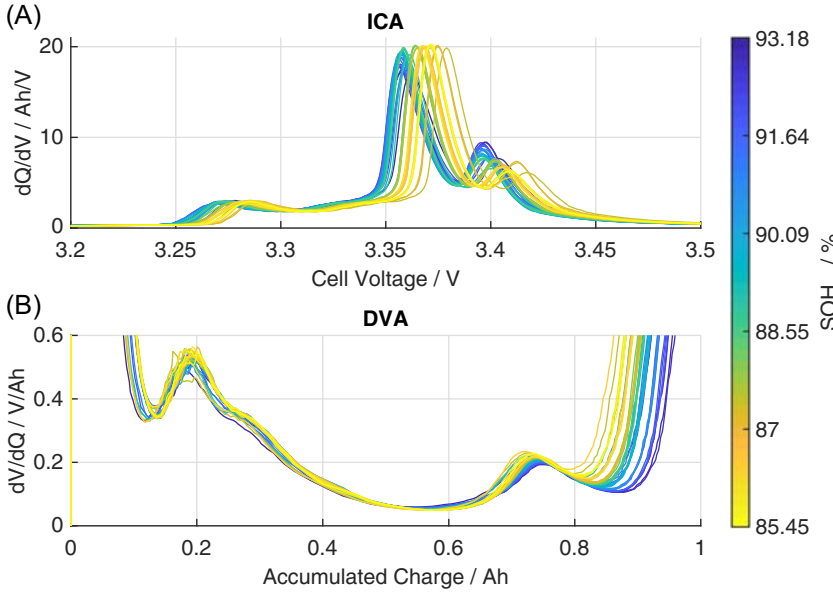


Figure 7.12 The course of the differential curves of the (A) ICA and (B) DVA during a C/2 of a cyclically aged Li-ion battery (graphite anode/LFP cathode). *DVA*, Differential voltage analysis; *LFP*, Lithium Iron Phosphate. Please see the online version to view the color image of the figure.

4. Calculate and filter the differential curves (dV/dQ) based on the measurements.
5. Apply feature detection algorithm, that is, a peak detection algorithm, to extract the features. Based on the scenarios, different features may be extracted and used. Since the features themselves do not indicate the SOH_C, they will be further processed.
6. Apply a mapping function that relates the features with the SOH_C. Typically, the reference is represented by a Look-Up-Table that is based on the correlation between features and SOH_C, extracted from existing cyclic aged battery data.

As depicted in Fig. 7.13, the real SOH_C has strong correlations with DVA and ICA features; for example, the distance of two features or the height of a feature. The correlations also depend on the temperature. Higher charging currents will affect the estimation accuracy. However, this method can generally achieve 5% SOH accuracy when charging at C/2 or less.

7.5 Cloud-based thermal runaway prediction

7.5.1 Cause and effects of thermal runaway

One significant disadvantage of batteries is the narrow operating temperature range. The safety and stability of the battery cells are dependent on keeping interior temperatures under certain limits. A thermal runaway can occur if the temperature

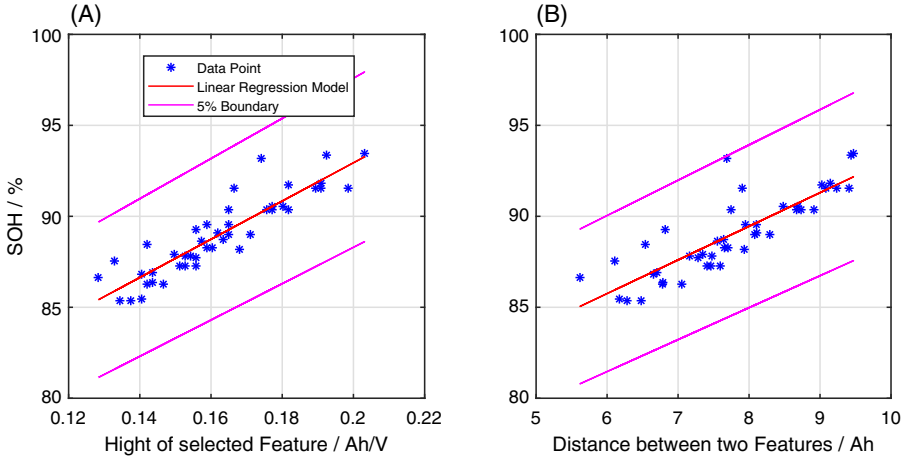


Figure 7.13 Correlation of selected features with capacity fade: (A) height of selected feature and (B) distance between two features. Please see the online version to view the color image of the figure.

surpasses the critical level, killing the battery or, even worse, causing a fire. Thermal runaway is a chain reaction that can be very difficult to stop once it has begun within a battery cell. During a thermal runaway, the temperature rises incredibly fast (milliseconds), and temperature can be higher than 752°F/400°C. At such elevated temperatures, electrolytes in the battery cell can be vaporized and combustive when exposed to oxygen. Such battery fires are hard to extinguish with conventional ways.

The heat generated by the electrochemical reactions is critical as it can lead to thermal runaway. The heat generation is caused by chemical/electrochemical reactions and joule heating inside the battery. Radiation and convection dissipate heat to the surroundings. The process of thermal runaway can be explained by the plot Fig. 7.14. The heat generation because of an exothermic reaction assuming Arrhenius law, an exponential function, is shown in curved line 4. In comparison, the heat dissipation is represented by straight lines, which follow Newton's cooling law at different coolant temperatures. For the lithium-ion battery, curve 4 is the combined results of reactions in the cell during the thermal runaway process and the energy balance between the heat generation. Heat dissipation is shown as Eq. (7.5):

$$\frac{\partial\left(\rho C_p T\right)}{\partial t} = -\nabla(k\nabla T) + Q_{\text{ab-chem}} + Q_{\text{joul}} + Q_S + Q_P + Q_{\text{ex}} + \cdots, \tag{7.5}$$

where $\rho\left(\text{gcm}^{-3}\right)$ is the composite/average density of the battery, $C_p\left(\text{Jg}^{-1}\text{K}^{-1}\right)$ is the composite/average heat capacity per unit mass under constant pressure, T(K) is the temperature, t(s) is the time, and $k\left(\text{Wcm}^{-1}\text{K}^{-1}\right)$ is the thermal conductivity.

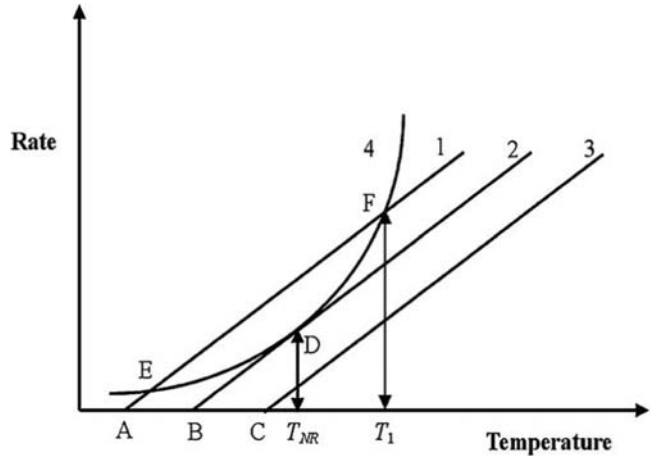


Figure 7.14 Thermal runaway explanation based on heat generation and dissipation models [41].

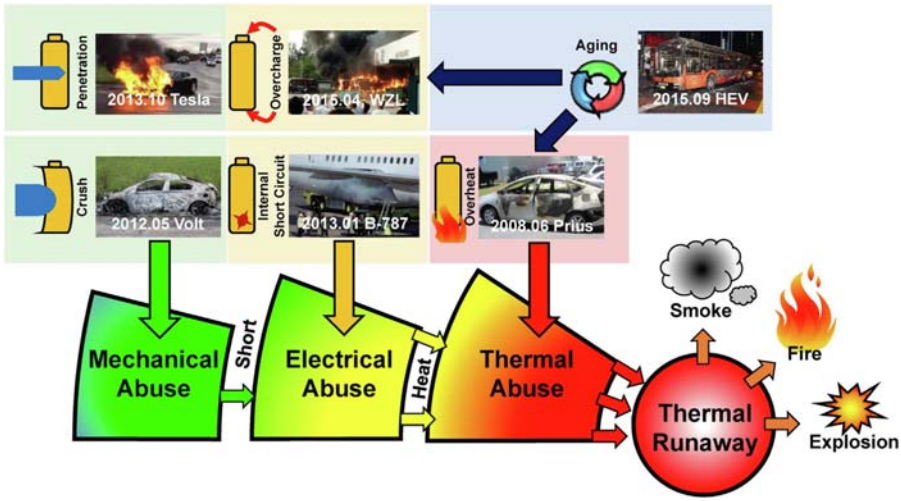


Figure 7.15 Abuses that cause thermal runaway [42].

$Q_{\text{ab-chem}}$ is the abuse chemical reaction in the battery, Q_{joul} is Joule heat, Q_s is the entropy heat, Q_P is the overpotential heat, and Q_{ex} is the heat exchange between the system and the ambient.

Generally, thermal runaway can be triggered by various types of abuse in a battery shown in Fig. 7.15 [42], which are described in the following sections.

Internal short circuit: caused by physical damage to the battery or poor battery maintenance.

Mechanical abuse: Vehicle collision and consequent crush or penetration of the battery pack are the typical conditions for mechanical abuse.

Electrical abuse

- Overcharging: The voltage that exceeds the maximum safety operation voltage range will damage the battery and lead to thermal runaway. Because of the extra energy filled into the battery during overcharge, the overcharge-induced TR can be more severe than other abuse conditions.
- Rapid charging can lead to excessive currents, therefore, causing thermal runaway.
- External short circuit: External short circuit happens when the electrodes with voltage difference are connected by conductors, which could also kick off the TR chain reaction.

Thermal abuse

- Over/under temperatures: Either the low or high side of the safety ranges degrades battery health, leading to irreversible damage that may eventually trigger the TR reaction.

7.5.2 Methods for thermal runaway detection

For typical batteries applications, including microgrids and electric vehicles, cells are connected and packed in modules and packs. Suppose one or a few cells experience thermal runaway due to the limited space for heat exchange. In that case, the heat will rapidly go up, leading to thermal runaway propagation among all surrounding batteries. Therefore it's essential to detect thermal runaways at an early stage to ensure safety. Lithium-ion batteries may experience voltage and current anomalies, temperature rises, or gas ventings during the thermal runaway process. Those are the indicators that can be detected at the early stage [43]. Methods of thermal runaway detection include:

Terminal voltage. The terminal voltage can be detected by using voltage sensors within the BMS.

Mechanical deformation. Mechanical deformation can be detected by creepage distance sensors.

Internal temperature. The core temperature directly represents the thermal condition within batteries, it can be either:

- measured by temperature sensor inserted in the batteries or
- estimated based on the measured surface temperature of batteries.

Gas component. Some gas components can be identified during the thermal runaway process, such as carbon monoxide, hydrocarbons, and hydrogen. Gas sensors such as thermal conductivity detectors (TCD) can be used for this purpose.

7.5.3 Data-driven thermal anomaly detection

Here we give a cloud-based and data-driven method for detecting battery thermal anomalies [44]. Because that this method is based on the measurements' shape similarities, which is less affected by cell deterioration or environmental variation, it is robust to battery aging or environment variations. As a result, this method can be applied to different battery configurations. The shape-based distance [Eq. (7.6)]

measurement handles the asynchronous data issue. It also needs very little reference data. This method is based on K-shape clustering [45]

$$\mathrm{SBD}(\vec{x}, \vec{y}) = 1 - \max_{\omega} \left(\frac{CC_{\omega}(\mathbf{x}, \mathbf{y})}{\sqrt{R_0(\mathbf{x}, \mathbf{x}) R_0(\mathbf{y}, \mathbf{y})}} \right), \tag{7.6}$$

where $\vec{x}, \vec{y}$ are two time series measurements that used for comparing similarity, and R_0 the Rayleigh quotient.

7.5.3.1 Workflow

As depicted in Fig. 7.16, the proposed anomaly detection method contains the following steps. At first, data is continuously buffered and segmented. During the preprocessing stage, invalid/faulted data points are removed. Signals are normalized. Segments with static signals are filtered out. During the anomaly confirmation stage, the K-shape algorithm is applied to each segment for the distances ($\mathrm{SBD}(x_i, c_j)$) for each cluster. Two criteria are used for determining anomaly. (1) when at least one of the measurements change the membership and (2) when no change was found in cluster membership, we check for any noticeable increase in the fitting errors. During each iteration, the *i*th cluster is compared to the reference cluster, which captures the accumulated, long-term changes that result from anomalies caused by gradual deterioration. Such as thermal anomalies caused by increased battery impedance. It's also compared to the predecessor for anomalies that developed abruptly, such as short circuit. In the final stage of anomaly isolation, we use the change of membership or increase in fitting error to isolate the signals that caused the anomaly.

7.5.3.2 Case study

We apply the proposed anomaly detection method to EV batteries. The data was collected and transmitted from an onboard BMS. As shown in Fig. 7.17A, temperature measurement from sensor #13 increased to over 70°C on October 30. The onboard BMS detects the overtemperature anomaly around 3:45 pm, during which the temperature was over 55°C. Meanwhile, the proposed method was able to detect anomalies around 2:15 p.m., which is about 90 minutes earlier. The detailed comparisons are illustrated in Fig. 7.17B. As it shows, the proposed method detects the anomaly when sensor #13 just started to behave differently from the other measurements. Fig. 7.17C is the shape plot of the segment that detects the anomaly. In this figure, sensor #13 is flagged as the outlier for its rising shape.

7.6 Conclusion

In this chapter, we present a battery cloud (cloud-BMS) which is aimed at improving battery performance, safety, and economy by utilizing cloud computing and the

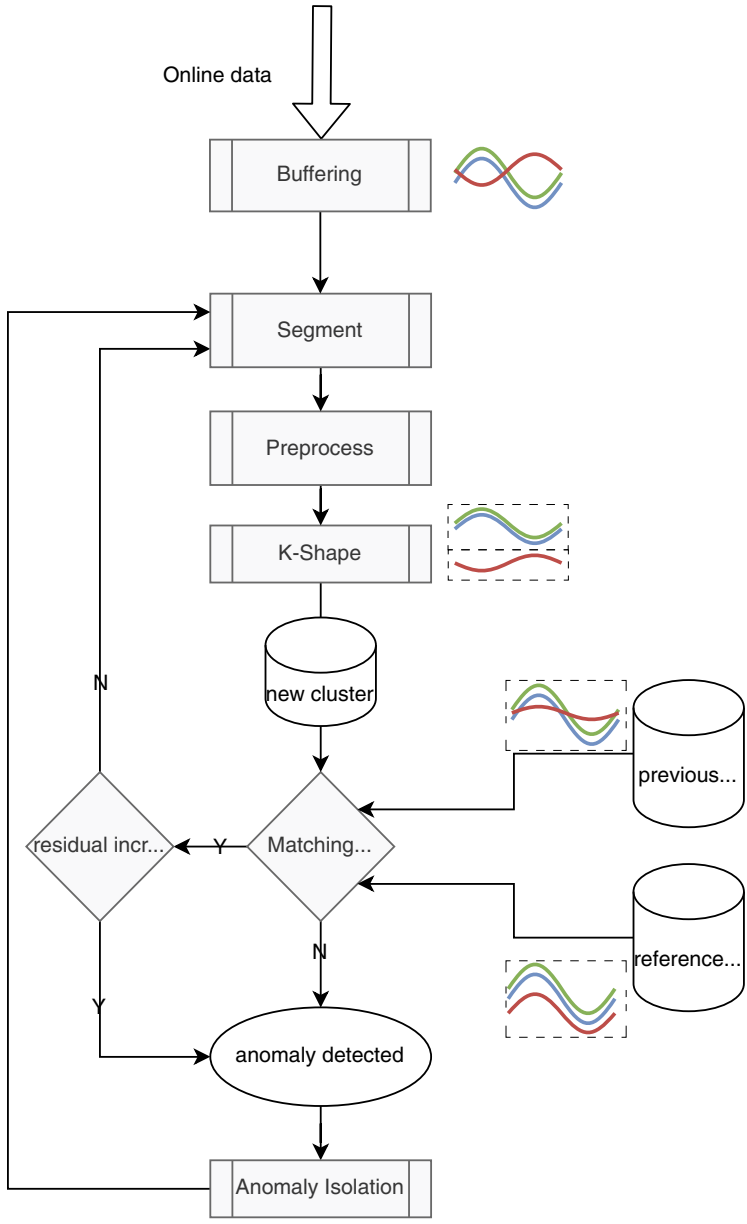
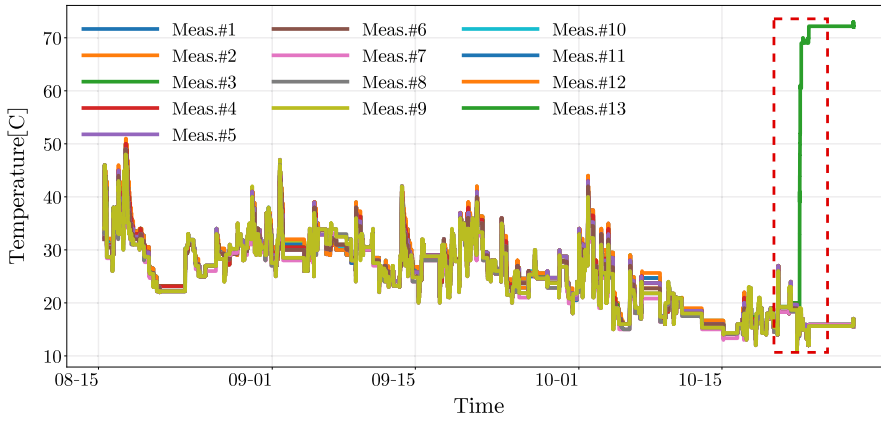
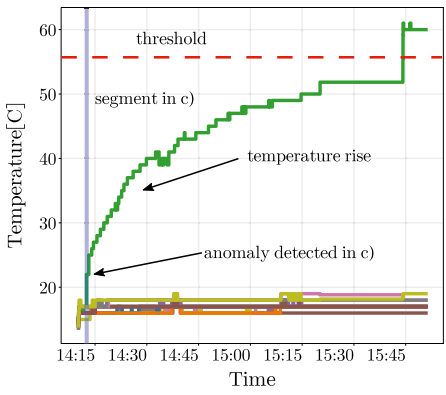


Figure 7.16 Flowchart for the thermal anomaly detection algorithm.

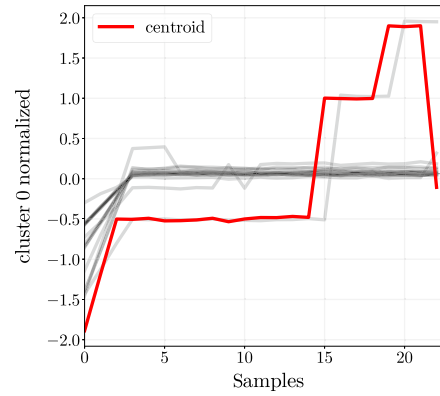
IoT. The major component of a battery cloud includes the data sources during the stages of the battery life cycle, the different choices of databases, and deployment for battery data and data visualization. In addition, we discuss core algorithms for



(A) two months of temperature signals, over-temperature highlighted



(B) anomaly detected 90min ahead



(C) one of the signal has different shape

Figure 7.17 Test case (A) temperature measurement which shows the overtemperature fault. (B) The zoom-in view of the fault occurrence, this method detects the temperature anomaly 90 min before the onboard BMS. (C) Further zoom-in view of the segment's shapes plot where the anomaly is detected, which is also highlighted in (B).

the battery cloud. Firstly, an ANN is trained with cloud battery data for SOC estimation. The ANN is eventually deployed to the onboard BMS and tested on the vehicle. The successful testing results show that cloud battery data is essential for developing advanced battery algorithms. Secondly, we discuss the degradation mechanisms of battery health and different algorithms for SOH. We develop an SOH estimation method based on DVA/ICA, which shows $<5\%$ accuracy under different operating temperatures. At last, we review one important safety issue for batteries, thermal runaway. Its cause and effects are discussed. A data-driven battery anomaly detection method is developed to give early warnings.

References

[1] B. Dunn, H. Kamath, J.-m Tarascon, Electrical energy storage for the grid: a battery of choices, Sci. Mag. 334 (6058) (2011) 928−936.

[2] Pacific Northwest National Laboratory, "Lithium-ion battery (LFP and NMC)," 2022. [Online]. Available: https://www.pnnl.gov/lithium-ion-battery-lfp-and-nmc

[3] T. Lombardo, M. Duquesnoy, H. El-Bouysidy, F. Årén, A. Gallo-Bueno, P.B. Jørgensen, et al., Artificial intelligence applied to battery research: hype or reality? Chem. Rev. (2021).

[4] L.D. Xu, W. He, S. Li, Internet of things in industries: a survey, IEEE Trans. Ind. Inform. 10 (4) (2014).

[5] "Voltaiq." [Online]. Available: https://www.voltaiq.com/

[6] "How Gotion monitors its EV battery solution with InfluxDB, Grafana and AWS." [Online]. Available: https://www.influxdata.com/resources/how-gotion-monitors-its-ev-battery-solution-with-influxdb-grafana-and-aws/

[7] J. Schnell, C. Nentwich, F. Endres, A. Kollenda, F. Distel, T. Knoche, et al., Data mining in lithium-ion battery cell production, J. Power Sources 413 (2019) 360−366. Available from: https://doi.org/10.1016/j.jpowsour.2018.12.062. no. October 2018.

[8] Apache, "Apache Hadoop," 2022. [Online]. Available: https://hadoop.apache.org/, 2022 (accessed 11.10.22)

[9] Amazon, "Amazon Web Service," 2022. [Online]. Available: https://aws.amazon.com/, 2022 (accessed 11.10.22)

[10] Microsoft, "Microsoft Azure," 2022. [Online]. Available: https://azure.microsoft.com/, 2022 (accessed 11.10.22)

[11] Google, "Google Cloud Platform," 2022. [Online]. Available: https://cloud.google.com/, 2022 (accessed 11.10.22)

[12] Cloudera, 2022. [Online]. Available: https://www.cloudera.com/, 2022 (accessed 11.10.22)

[13] influxdata, "Influxdb," 2022. [Online]. Available: https://www.influxdata.com/products/influxdb-overview/, 2022 (accessed 11.10.22)

[14] W. Li, M. Rentemeister, J. Badeda, D. Jöst, D. Schulte, D.U. Sauer, Digital twin for battery systems: cloud battery management system with online state-of-charge and state-of-health estimation, J. Energy Storage 30 (April) (2020) 101557. Available from: https://doi.org/10.1016/j.est.2020.101557 [Online]. Available.

[15] A. Abdollahi, J. Li, X. Li, T. Jones, A. Habeebullah, "Voltage-based state of charge correction at charge-end," in *2021 IEEE Vehicle Power and Propulsion Conference (VPPC)*, 2021, pp. 1−6.

[16] E. Chemali, P.J. Kollmeyer, M. Preindl, A. Emadi, State-of-charge estimation of Li-ion batteries using deep neural networks: a machine learning approach, J. Power Sources 400 (June) (2018) 242−255. Available from: https://doi.org/10.1016/j.jpowsour.2018.06.104 [Online].

[17] M.A. Hannan, M.S. Lipu, A. Hussain, A. Mohamed, A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: challenges and recommendations, Renew. Sustain. Energy Rev. 78 (2017) 834−854. Available from: https://doi.org/10.1016/j.rser.2017.05.001. no. August 2016.

[18] C.R. Birkl, M.R. Roberts, E. McTurk, P.G. Bruce, D.A. Howey, Degradation diagnostics for lithium ion cells, J. Power Sources 341 (2017) 373−386.

[19] J. Vetter, P. Novák, M.R. Wagner, C. Veit, K.C. Möller, J.O. Besenhard, et al., Ageing mechanisms in lithium-ion batteries, J. Power Sources 147 (1−2) (2005) 269−281.
[20] M. Dubarry, C. Truchot, B.Y. Liaw, Synthesize battery degradation modes via a diagnostic and prognostic model, J. Power Sources 219 (2012) 204−216.
[21] M.M. Kabir, D.E. Demirocak, "Degradation mechanisms in Li-ion batteries: a state-of-the-art review," 2017.
[22] P. Verma, P. Maire, P. Novák, A review of the features and analyses of the solid electrolyte interphase in Li-ion batteries, Electrochim. Acta 55 (22) (2010) 6332−6341 [Online]. Available. Available from: http://www.sciencedirect.com/science/article/pii/S0013468610007747.
[23] D. Aurbach, B. Markovsky, I. Weissman, E. Levi, Y. Ein-Eli, On the correlation between surface chemistry and performance of graphite negative electrodes for Li ion batteries, Electrochim. Acta 45 (1) (1999) 67−86 [Online]. Available. Available from: http://www.sciencedirect.com/science/article/pii/S0013468699001942.
[24] P. Keil, A. Jossen, "Aging of lithium-ion batteries in electric vehicles: Impact of regenerative braking," pp. 41−51, 2015. [Online]. Available: https://mediatum.ub.tum.de/node?id = 1355829
[25] M. Broussely, P. Biensan, F. Bonhomme, P. Blanchard, S. Herreyre, K. Nechev, et al., Main aging mechanisms in Li ion batteries, J. Power Sources 146 (1−2) (2005) 90−96 [Online]. Available. Available from: http://www.sciencedirect.com/science/article/pii/S0378775305005082.
[26] P. Arora, R.E. White, M. Doyle, Capacity fade mechanisms and side reactions in lithium-ion batteries, J. Electrochem. Soc. 145 (10) (1998) 3647−3667 [Online]. Available. Available from: https://iopscience.iop.org/article/10.1149/1.1838857.
[27] X. Han, L. Lu, Y. Zheng, X. Feng, Z. Li, J. Li, et al., A review on the key issues of the lithium ion battery degradation among the whole life cycle, eTransportation 1 (2019) 100005.
[28] T. Waldmann, S. Gorse, T. Samtleben, G. Schneider, V. Knoblauch, M. Wohlfahrt-Mehrens, A mechanical aging mechanism in lithium-ion batteries, J. Electrochem. Soc. 161 (10) (2014) A1742−A1747 [Online]. Available. Available from: https://iopscience.iop.org/article/10.1149/2.1001410jes.
[29] R. Korthauer, Handbuch Lithium-Ionen-Batterien, Springer Berlin Heidelberg, 2013.
[30] USABC, "Electric vehicle battery test procedures - Rev. 2," 1996. [Online]. Available: http://www.uscar.org/commands/files_download.php?files_id = 73
[31] E. Wood, M. Alexander, T.H. Bradley, Investigation of battery end-of-life conditions for plug-in hybrid electric vehicles, J. Power Sources 196 (11) (2011) 5147−5154 [Online]. Available. Available from: http://www.sciencedirect.com/science/article/pii/S037877531100379X.
[32] V. Marano, S. Onori, Y. Guezennec, G. Rizzoni, N. Madella, "Lithium-ion batteries life estimation for plug-in hybrid electric vehicles," in *5th IEEE Vehicle Power and Propulsion Conference, VPPC '09*, 2009, pp. 536−543.
[33] Y. Zhang, C.Y. Wang, X. Tang, Cycling degradation of an automotive LiFePO4 lithium-ion battery, J. Power Sources 196 (3) (2011) 1513−1520 [Online]. Available. Available from: https://pennstate.pure.elsevier.com/en/publications/cycling-degradation-of-an-automotive-lifeposub4sub-lithium-ion-ba.
[34] A. Tomaszewska, Z. Chu, X. Feng, S. O'Kane, X. Liu, J. Chen, et al., Lithium-ion battery fast charging: a review, eTransportation 1 (2019) 100011.

[35] R. Xiong, L. Li, J. Tian, Towards a smarter battery management system: a critical review on battery state of health monitoring methods, J. Power Sources 405 (2018) 18−29.
[36] M. Berecibar, I. Gandiaga, I. Villarreal, N. Omar, J. Van Mierlo, P. Van Den Bossche, Critical review of state of health estimation methods of Li-ion batteries for real applications, Renew. Sustain. Energy Rev. 56 (2016) 572−587.
[37] A. Eddahech, O. Briat, J.M. Vinassa, Determination of lithium-ion battery state-of-health based on constant-voltage charge phase, J. Power Sources 258 (2014).
[38] M. Dubarry, B.Y. Liaw, Identify capacity fading mechanism in a commercial LiFePO4 cell, J. Power Sources 194 (1) (2009) 541−549. 10.
[39] M. Dubarry, B.Y. Liaw, M.S. Chen, S.S. Chyan, K.C. Han, W.T. Sie, et al., Identifying battery aging mechanisms in large format Li ion cells, J. Power Sources 196 (7) (2011) 3420−3425.
[40] X. Han, M. Ouyang, L. Lu, J. Li, A comparative study of commercial lithium ion battery cycle life in electric vehicle: capacity loss estimation, J. Power Sources 268 (2014) 658−669 [Online]. Available. Available from: http://www.sciencedirect.com/science/article/pii/S0378775314009756.
[41] Q. Wang, P. Ping, X. Zhao, G. Chu, J. Sun, C. Chen, Thermal runaway caused fire and explosion of lithium ion battery, J. Power Sources 208 (2012) 210−224.
[42] X. Feng, M. Ouyang, X. Liu, L. Lu, Y. Xia, X. He, Thermal runaway mechanism of lithium ion battery for electric vehicles: a review, Energy Storage Mater. 10 (2018) 246−267.
[43] Z. Liao, S. Zhang, K. Li, G. Zhang, T.G. Habetler, A survey of methods for monitoring and detecting thermal runaway of lithium-ion batteries, J. Power Sources 436 (2019) 226879.
[44] X. Li, J. Li, A. Abdollahi, T. Jones, A. Habeebullah, Data-driven thermal anomaly detection for batteries using unsupervised shape clustering, 2021 IEEE 30th International Symposium on Industrial Electronics (ISIE) (2021). Available from: https://doi.org/10.1109/ISIE45552.2021.9576348.
[45] J. Paparrizos, L. Gravano, "K-shape: efficient and accurate clustering of time series," in Proceedings of the ACM SIGMOD International Conference on Management of Data, vol. 2015-May. Association for Computing Machinery, 5 2015, pp. 1855−1870.

Applicability of federated learning for securing critical energy infrastructures

8

Yogesh Beeharry[1], *Vandana Bassoo*[1] *and Nitish Chooramun*[2]
[1]Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Mauritius, Réduit, Mauritius, [2]Department of Software and Information Systems, Faculty of Information, Communication and Digital Technologies, University of Mauritius, Réduit, Mauritius

Chapter Outline

8.1 Introduction

The energy grid, which was previously monopolized by non-renewables, has witnessed unprecedented changes with the incorporation of renewable energy sources, such as solar, wind, biomass, and tidal. The main reason behind this transformation is climate change and the need to take urgent actions in line with the United Nations sustainable development goal (SDG) 13. SDG 13 has set a number of targets to combat climate change. Some of these targets are strengthening resilience and adaptive capacity to climate-related hazards and natural disasters in all countries; integrating of climate change measures into national policies, planning and

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00003-3

strategies; building knowledge and capacity to meet climate change; and promoting mechanisms to raise capacity for effective climate change-related planning and management.

These critical energy infrastructures (CEIs) are adopting digitization at an accelerated pace together with the inclusion of the Internet of Things (IoT) in view of bringing smartness in all aspects of the different systems involved in the proper functioning of the architecture. Smart grids provide considerable benefits over traditional power systems through improved reliability, availability, and efficiency [1]. Essentially, within such grids, intelligent systems are deployed to control and monitor energy generation, transmission, distribution, and storage. Additionally, machine learning (ML) mechanisms have gained tremendous interest and popularity in various fields over the past decade. This has engendered automated mechanisms to be brought into being and deployed in CEIs as well. Although the digitization process and adoption of ML in CEIs aid in easing human efforts for accomplishing various tasks, it cannot be denied that it comes along with possibilities of security breaches and cyberattacks. It is of paramount importance to research the different security vulnerabilities that can be exploited by attackers and devise robust mechanisms for countering them.

Moreover, the voluminous data in CEIs calls for big data infrastructures. As in any other application domain where big data is concerned, having a centralized data warehouse involves serious burdens on the communication links in terms of bandwidth consumption and the data warehouse in terms of the storage capacity requirements. As such, ingenious developments in the intersecting area of ML and parallel computing domains have given rise to the concept of federated learning (FL), which addresses the problem of having a centralized data warehouse. However, this new concept still needs a lot of research in studying the security vulnerabilities and devising robust defense mechanisms before being fully fit for deployment in CEIs.

The main motivation of this work is to channel the attention of the readers of this book into:

- the security and privacy concerns involved in modern interconnected networks/ smart grids,
- the evolution of ML into FL in this setup environment, and
- the possible enhancements that can be made to the FL approach in this context.

Thus, the main objectives of this chapter are:

- to present a review of FL and its applications in security and privacy and
- to present a demonstration case involving the implementation of a simulated model of FL for enhancing the security of systems.

Typically, most research concerning strategies for securing CEIs includes reviews of techniques and evaluation studies. However, our work differs from previous works with the following significant contributions:

- presenting a demonstration case using FL for enhancing the security of systems and
- providing insights regarding security vulnerabilities and possible mitigation strategies.

This chapter is organized as follows: Section 8.2 presents a review of cyberattacks in smart grids. In Section 8.3, a review of FL and its challenges is presented. This is followed by a demonstration case involving the use of FL for enhancing cyber-security in Section 8.4. In Section 8.5, we present the simulation results. Insights into FL security countermeasures are provided in Section 8.6, followed by concluding remarks in Section 8.7.

8.2 Review of cyberattacks in smart grids

Information and communication technologies, particularly the IoT, are set to become the core platform of smart grids. These grids enable the real-time monitoring of electrical parameters, including voltage, current, power, and frequency, while providing remote access and reading capabilities.

Moreover, smart grids typically consist of various technologies, including advanced metering infrastructures, energy storage mechanisms, automated power outage management, renewable energy sources, and electric vehicles. These systems, coupled with the data transmission and communication infrastructures, add to the complexity of smart grids. Furthermore, smart grid domains comprise multiple communicating components, namely; markets, operations, service providers, customers, bulk generation, distribution, and transmission [2]. This varied ecosystem of technologies and components makes smart grids, inherently cyber-physical systems, particularly vulnerable to various cyberattacks. The following section presents an overview of major cyberattacks on power systems and smart grids.

8.2.1 Major cyberattacks in power systems and smart grids

Given the heterogeneity of systems used in smart grids and the volume of data communicated across the various systems, such grids are typically prone to cyberattacks. The nature of these attacks can be varied; for instance, it could involve attacking the system components for manipulating electricity bills, end users or consumers trying to change their power consumption information, or even the total collapse of entire systems.

In 2009, the US electric grid was hacked by cyberspies, and it was reported that hidden software could be used to cause power disruptions by attackers. It is believed that the spies were aiming to map to electrical grid infrastructure rather than cause immediate damage [3].

In 2010, a major cyber-security incident occurred in the Bushehr nuclear power plant in Iran, whereby the Stuxnet malware was used to manipulate control systems, which destroyed more than 1000 centrifuges [4]. This malware was introduced via an infected USB drive to exploit SCADA systems. It was able to identify the target control system, update itself and cause the centrifuges to malfunction [2].

A major cyber-security incident occurred in the Ukrainian power companies, whereby remote cyber intrusions were used to create unscheduled power outages

that impacted around 225,000 customers. It was reported that the BlackEnergy and KillDisk malware were used during these attacks. Moreover, the attack entailed the deletion of selected files from several systems, which, in turn, hindered their operation [5].

In March 2019, the North American Electric Reliability Corporation reported that a cyberattack on the US grid had caused a utility company to lose communication with some of its systems. A firewall vulnerability was exploited, which led to the unexpected reboots of multiple devices, thus causing communication outages [6,7]. A summary of the major cyberattacks on CEIs is presented in Table 8.1.

Given the impending threats to CEIs, numerous techniques and strategies are being devised to enhance the smart grids' resilience and their interconnecting components. One particular area that has gained momentum recently is the application of ML techniques, in particular FL, for securing grid infrastructures. These are illustrated in the next section of this article.

8.2.2 Suitability of Internet of Things-based technologies in modern grids

According to the United Nations SDG, ensuring access to reliable, sustainable, and modern energy remains a prime area of focus. As such, researchers, energy companies, and practitioners have been exploring the conversion of modern energy grids into smart grids [8]. IoT technologies can harness the capabilities of various sensing, actuation, and communication technologies in order to automate and integrate the core processes within the energy supply chain [9].

Advanced sensing mechanisms can be used to gather data from different grid assets in real-time, and IoT communication protocols with strong inbuilt security mechanisms, such as constrained application protocol can relay the data to operators for improved decision making related to the operational performance of the smart grid [10,11]. Moreover, IoT technologies have the potential to be used in automated threat mitigation systems. Such systems use data aggregation and analytics mechanisms coupled with intelligent systems to detect any anomalies in energy distribution and efficiency or even potential failures as a result of security threats [12].

Other mechanisms that have been proposed to improve cyber-security for smart grids include the principle of defense-in-depth [13]. This principle incorporates different measures for device and application security, network security, physical security, and policies. With regard to device and application security, IoT technologies can be used to gather data about the configuration of devices in the grids and detect insecure configurations and runtime vulnerabilities [13]. Likewise, changes in memory usage and modifications of the firmware of devices can be detected and reported to grid operators. Moreover, at the network level, IoT technologies can be used for implementing intrusion detection systems that can detect, as well as block, unwanted or suspicious network activities. For physical security, IoT technologies can be used to implement smart surveillance systems that can provide alerts in cases of unauthorized access to premises.

Table 8.1 Major cyberattacks on critical energy infrastructures.

No.	Security incident	Year	Type	Location	Impact/description	References
1.	US electric grid	2009	Power generation and distribution	United States	Mapping of the US electric grid by cyberspies. Although no damage was done, it was reported that the backdoors to the system could be opened during crisis times.	[3]
2.	Bushehr nuclear power plant	2010	Power generation	Iran	Stuxnet malware used to manipulate control systems caused the destruction of more than 1000 centrifuges.	[4,2]
3.	Ukrainian power companies	2015	Power distribution	Ukraine	Remote cyber intrusions at three electric power distribution companies causing unscheduled power outages and impacting 225,000 customers.	[5]
4.	Power grid cyberattack	2019	Communication	Western United States	Loss of communication with multiple power generation sites. Firewalls rebooting and going offline for nearly 10 hours	[6,7]

8.3 Federated learning and challenges

In this section, an overview of FL and the corresponding challenges is provided.

8.3.1 Federated learning

FL is a decentralized ML technique introduced by Google in the year 2016 [14]. It aims at addressing two main challenges, which are privacy and resource constraints. Efficient ML algorithms require a high volume of data for training purposes. Nowadays, large datasets are available but are generally stored in isolated systems. In centralized ML techniques, the data is transferred to a cloud platform or central server for processing. The transfer of large amounts of data is sometimes infeasible due to unstable Internet connections and the asymmetric nature of broadband Internet. Typically, the uplink speed is less than that of the downlink. Moreover, the uploading of a lot of data can clog the network and increase latency.

Privacy and new legislations are another set of challenges faced by centralized ML techniques. The 2008 General Data Protection Regulation and other regulations have been implemented to protect individuals' privacy and data security. Nowadays, integrating data across institutions and sharing raw data with third-party organizations are complicated [14].

FL uses a decentralized approach and conducts training on individual devices on which the data is generated. The technique aims at exploiting the unused processing power of many modern edge devices. After the training, each device transfers only the local model parameters to a central unit. The latter uses those parameters and an aggregation algorithm to revise the global model. The updated model is then fed back to individual devices for future use. Fig. 8.1 shows an FL model. The raw data is not transferred and remain on the original devices [15]. The enhanced privacy may encourage more users to participate in collaborative training.

8.3.2 Challenges of federated learning

FL is a relatively new technique that still presents some challenges. Statistical and system heterogeneity are discussed in this section, whereas security threats are discussed in Section 7.3.3.

8.3.2.1 Statistical heterogeneity

In FL, the various devices may generate data that is not reflective of the distribution of the entire dataset leading to a nonindependent and identically distributed format. Moreover, the datasets are considered unbalanced as the amount of data collected by each device may vary. In [16], the authors propose a few methods to address the challenges of statistical heterogeneity. The methods focus on the global model, consider preprocessing data, and modify the local training approach.

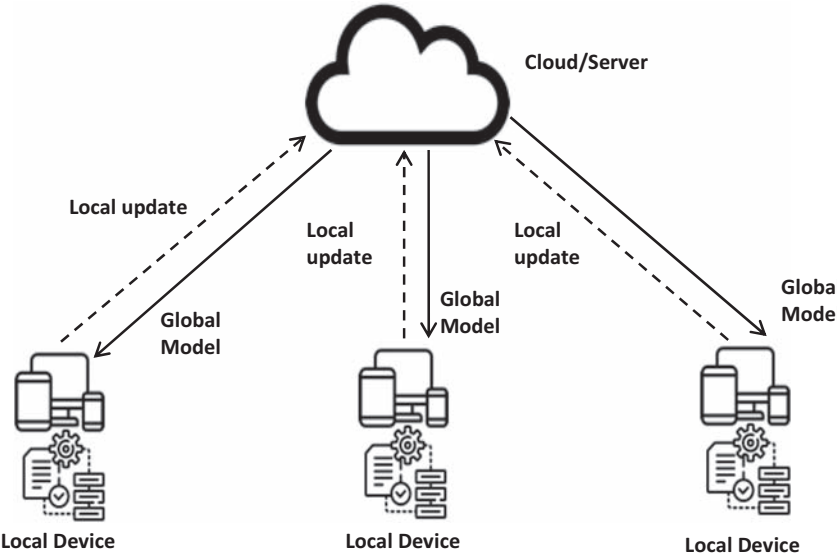


Figure 8.1 Federated learning model.

8.3.2.2 System heterogeneity

Distributed conventional ML is normally carried out in a data center on a set of homogenous machines with a robust communication network. However, FL uses a large number of heterogeneous devices to conduct local training over diverse networks. The network may not be stable at all times and lead to devices dropping off [17]. These devices have varying computing, energy, and storage resources leading to unequal training times. One possible approach to mitigate this problem is encouraging premium devices to participate in the training [16]. Nevertheless, robust FL methods should tolerate participating devices dropping off in the middle of a training iteration.

8.3.3 Survey of threats, attacks, and defense strategies

Numerous research works have been done, and many more are ongoing to identify potential security risks. The information about security threats, attacks, and defensive techniques in FL have been derived from reference [18] and are presented in Table 8.2.

Poisoning [19,20] is a security threat that deals with the tampering of the data or the model weights being exchanged during the FL process. It can be categorized into data poisoning/data injection [21], model poisoning [24–26], and data modification [27,28]. Data poisoning or data injection deals with incorporating malicious data points in the form of training data or model parameters, depending on where

Table 8.2 Security threats, attacks, and defensive techniques in federated learning (FL) domain.

Security threats, attacks in FL domain		**Defensive techniques for security vulnerabilities in FL**
Poisoning [19,20]	Data poisoning/data injection [21] Model poisoning [24−26] Data modification [27,28]	Sniper [22], data sanitization [23]
Inference attacks [19,20]		
Backdoor attacks [24,29]		Model pruning and fine-tuning [30,31]
Generative adversarial networks [32]		PDGAN [33]
Malicious server [34]		Secure FL [35], anomaly detection [36], Foolsgold [37]
Communication bottlenecks [38,39]		Communication bandwidth preserving [40,41], knowledge distillation [42], federated multitask learning [43]
Free-riding attacks [44]		Enhanced anomaly detection using autoencoders [45]
UnavailabilityEavesdroppingInterplay with data protection laws		Moving target defense [46]

the attack is taking place. Inference attacks [19,20] are mainly a privacy threat, but the impact is as severe as that caused by poisoning attacks. Research for corresponding countermeasures is ongoing in inference attacks, but anonymization techniques can be used. Backdoor attacks [24,29] are quite difficult and time-consuming to detect since it involves the injection of malicious tasks in existing models without altering the latter's accuracy. GAN-based attacks are mostly a combination of inference and poisoning attacks [32]. Malicious server attack is very dangerous in cross-device FL since model parameters can be easily extracted, and global models can be manipulated with undetectable malicious tasks before broadcasting to client devices. Communication bottleneck attacks significantly disrupt the FL ecosystem when having low communication bandwidth due to different flavors of denial of service attacks. Free-riding attacks [44] occur mainly in cases where ML models are deployed from crowdsourced information. In this case, clients not contributing to the training process will be leveraging the global model. They can, at any instant, have the ability to inject false updates without any training on local data. Unavailability is, to some extent, similar to free-riding attacks, but in this case, the client fails to contribute to the global model update. Eavesdropping occurs on weak communication channels between client and server where an

attacker can monitor traffic and extract data. The interplay with data protection laws usually has a low possibility of occurrence since a thorough analysis is conducted by configurators of the FL environment before being deployed into production. All the corresponding defensive mechanisms are also provided for each of the presently known attacks in the literature. However, there is ongoing research in detecting security threats, enhancing existing defensive mechanisms, and devising novel defense systems for existing and newly discovered security in the FL ecosystem. The advantages/strengths and drawbacks/weaknesses can be summarized as shown in Figs. 8.2 and 8.3.

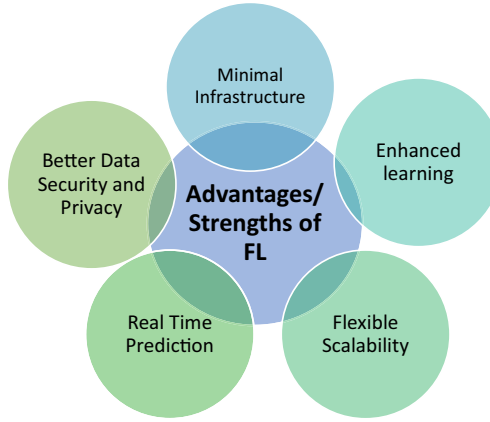


Figure 8.2 Advantages/strengths of federated learning.

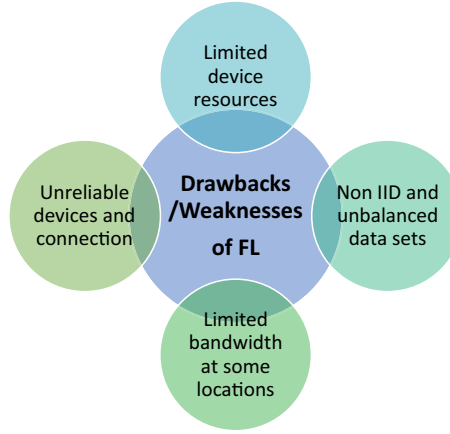


Figure 8.3 Drawbacks/weaknesses of federated learning.

8.4 Simulated system model

The simulations have been conducted using the Python programming language. More specifically, the PyGAD library is used for training a classification-based neural network using the genetic algorithm [47].

The parameters set in the mathematical model of a genetic algorithm-based neural network are as follows:

- number of neurons at the input layer: 78
- number of hidden layers: 2
- number of neurons in each hidden layer: 10
- number of neurons in the output layer: 2
- activation function for the neurons of the hidden layer: “relu”
- activation function for the neurons of the output layer: “softmax”

8.4.1 System architecture

The conventional FL model simulated is shown in Fig. 8.4. The individual models for each attack are learned locally, the model parameters are aggregated at the EDGE server, and the global model is then broadcasted to the plants.

The scenario shown assumes that the two plants (Plant 1 and Plant 2) have a local data store with preprocessed and labeled data ready for training an ML model. Instead of having a centralized data store, the idea of FL is to have a centralized model aggregation performed at the EDGE, as shown in Fig. 8.2. This technique avoids the hassle of transferring data, which burdens the communication link and

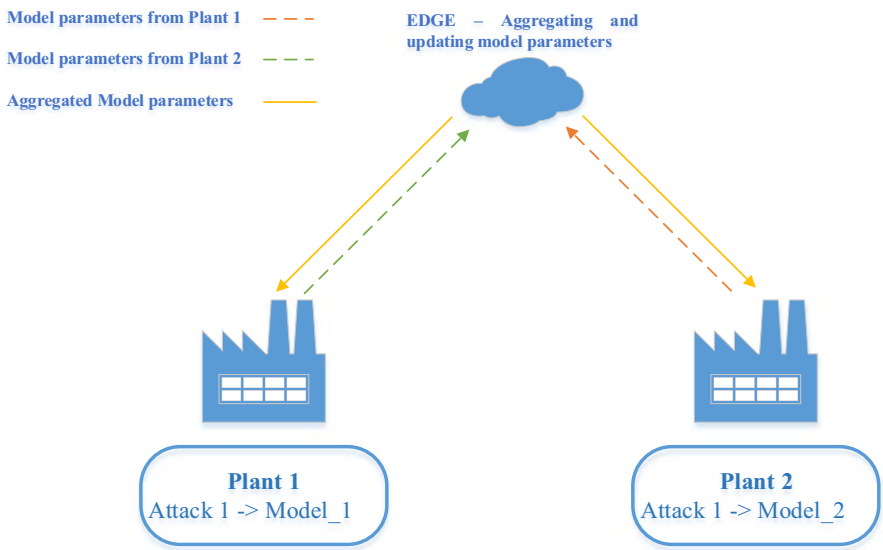


Figure 8.4 Simulated model for federated learning.

raises data privacy and security concerns during the transfer. Given that only the model parameters are being transferred, the risk for an attacker to access the data during that process on the communication link has a minuscule or zero probability.

The simulation is performed such that a multithreaded socket connection is set up with the initial model specified at the EDGE. The information about the model is then forwarded to the two respective plants once the connection is established. Locally, at the plants, the model is trained on the respective datasets. The parameters of which are then sent over to the EDGE for aggregation. The global model obtained is then broadcasted to the plants, and a comparison is made in terms of fitness with the previous local models. The model parameters are updated at the plants and aggregated at the EDGE until no more improvement in the trained model is observed. The process is then halted, the final model is sent over to the plants, and the socket connection is closed.

8.4.2 HAI dataset

In this chapter, the Hardware-in-Loop-based Augmented Industrial control system (HAI) security dataset [48–50] has been used to present the FL mechanism. The HAI dataset has been made available on repositories, such as GitHub and Kaggle, for research purposes geared toward anomaly detection in cyber-physical systems. Starting with three independent laboratory-scale testbeds comprising a boiler, turbine, and water-treatment component, a more complex system was devised later [50]. The latter incorporated a hardware-in-the-loop (HIL) simulator combining all three testbeds in a single system. The complete process architecture is described in the documentation of the HAI dataset [49,50]. The simulations performed were that of pumped-storage hydropower and thermal power generation. In a nutshell, the dataset consists of Industrial Control System data from both normal and anomalous conditions related to different types of cyberattacks. The sample data folder for the HAI dataset used has the characteristics shown in Table 8.3. The dataset globally consists of 78 feature columns and 4 columns for data labels representing the occurrence of an attack. An additional column for the timestamp is also available but is excluded at the data preprocessing stage. Furthermore, the predictive model is set to a binary classifier for simplicity, and thus a single column of attack label is used from the four provided columns in the dataset.

The dataset has a structure corresponding to a siloed data store. For simulating the scenario for FL, the data files have been rearranged and organized so that training data is received from two distinct plants, and a test dataset is used for the testing and validation of the federated model obtained. The breakdown of the data files is as shown in Table 8.4.

The breakdown shown in Table 8.4 has been performed with the aim:

- to have a balanced distribution of the amount of data being trained at both plants,
- to have a balance between the mix of normal anomalous data at both plants, and
- to have a balanced distribution of the attack counts for training at both plants and the testing.

Table 8.3 Characteristics of HAI dataset folder.

		Normal dataset		Attack dataset		
Folder name/ version	**Data points**	**Files**	**Interval**	**Files**	**Attack count**	**Interval**
HAI 21.03	78 points/sec	train1.csv train2.csv train3.csv	60 hours 63 hours 229 hours	test1.csv test2.csv test3.csv	5 20 8	12 hours 33 hours 30 hours
				test4.csv test5.csv	5 12	11 hours 26 hours

Table 8.4 Breakdown of data files.

Plant 1—Training data	**Plant 2—Training data**	**Test data**
train1.csv train2.csv test2.csv	train3.csv test3.csv test4.csv	test1.csv test5.csv –

During the simulation, the computer's hardware resources were not sufficient to handle the data sizes being processed in parallel. For proceeding with the proper running of the simulations, the redistribution and assignment of the data files were performed, as highlighted in Table 8.4.

8.5 Simulation results

The simulation results obtained are presented in this section. The simulations have been conducted using the Python programming language. More specifically, the PyGAD library is used for training a classification-based neural network using the genetic algorithm. The hardware used to perform the simulations has the specifications shown in Table 8.5.

8.5.1 Model fitness evolution

The evolution of the model fitness for one set of generations with the genetic algorithm is shown in Fig. 8.5.

The evolution of the fitness of the different local models at the respective plants is depicted in Fig. 8.3. It demonstrates how the fitness increases from approximately 50% to finally stabilize at around 97%. The final model is obtained when the fitness settles and remains fairly constant over successive iterations and until the condition for no further change is met. The confusion matrix representing the results obtained with the test dataset is shown in Fig. 8.6.

Table 8.5 Device specifications.

System type	64-bit operating system, ×64-based processor
Processor	Intel(R) Core(TM) i5−10210U CPU @ 1.60 GHz 2.11 GHz
Installed RAM	16.0 GB (15.8 GB usable)

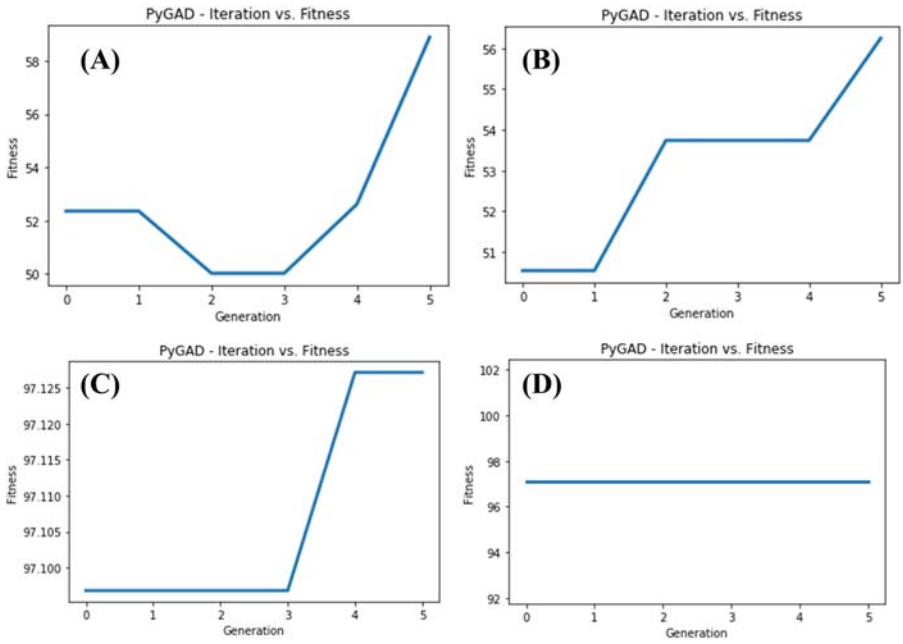


Figure 8.5 Model fitness evolution. (A) Evolution of fitness in the range 50%−58%. (B) Evolution of fitness in the range 51%−56%. (C) Evolution of fitness in the range 97.100%−97.125%. (D) Stabilised fitness between 97% and 98%.

8.5.2 Confusion matrix

The metric providing insight on the number of correct results that the model has managed to identify is defined as the accuracy and is given as:

$$\text{Accuracy} = \frac{T_p + T_n}{T_p + F_p + F_n + T_n} = \frac{132 + 132794}{132 + 2 + 2674 + 1332794} = 0.9803 \quad (8.1)$$

where T_p represents the true positive and is indicative of the "No Attack" labels predicted as "No Attack," F_p represents the false positive and is indicative of the "No Attack" labels predicted as "Attack," F_n represents the false negative and is indicative of the "Attack" labels predicted as "No Attack," T_n represents the true negative and is indicative of the "Attack" labels predicted as "Attack."

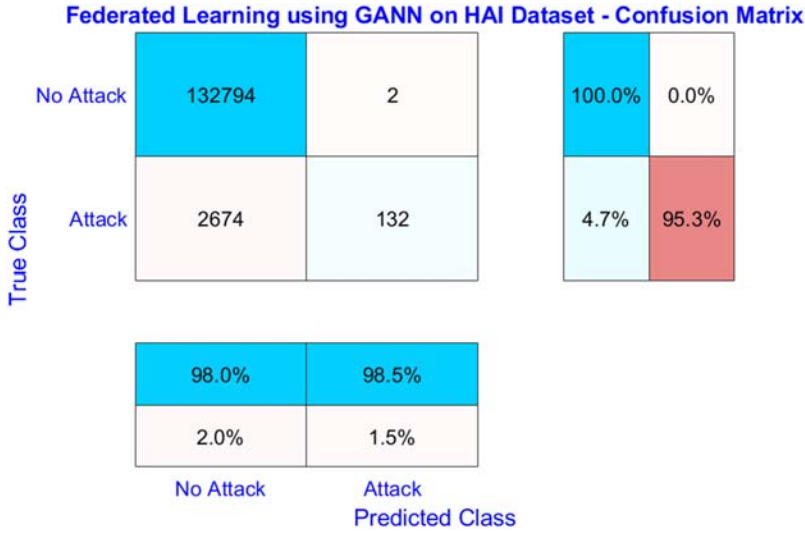


Figure 8.6 Confusion matrix for FL model prediction with the HAI test dataset. *FL*, Federated learning.

The precision metric represents the fraction of predicted attacks that have been correctly classified and is given as:

$$\text{Precision} = \frac{T_p}{T_p + F_p} = 0.9851 \tag{8.2}$$

The fraction of the correctly predicted "Attack" labels to the total number of "Attack" predicted classes is given by the recall:

$$\text{Recall} = \frac{T_p}{T_p + F_n} = 0.0470 \tag{8.3}$$

The specificity of the correctly predicted "No Attack" labels to the total number of "No Attack" predicted classes is given by the recall:

$$\text{Specificity} = \frac{T_n}{F_p + T_n} = 1.0 \tag{8.4}$$

The F-score measure, which enables the trade-off between precision and recall metrics by approximately averaging them, is given as:

$$\text{F} - \text{score} = \frac{2\text{x}T_p}{2\text{x}T_p + F_p + F_n} = 0.0898 \tag{8.5}$$

In this case, the F-score is very low, and one possible reason could be the larger number of "No Attack" labels in the test dataset, as can be seen from the confusion matrix. The model used can thus be further tuned for use in the FL ecosystem such that better accuracy and F-score are obtained.

8.6 Insights on federated learning security countermeasures

One loophole that can be intuitively spotted in the simulated system is that the socket connections are kept open until the final aggregated model is not obtained. Although access to the data is limited in this case, the possibility for an attacker to access the ML model parameters and make modifications can still not be pushed aside. In the advent of this scenario, modification of the model parameters will completely disrupt the proper functioning of the anomaly detection model itself. It may result in an increased number of false positives or false negatives.

One possible way to tackle this scenario would be to use ensemble models on top of the FL process. The single model parameters being transferred back and forth between the plants and the EDGE aggregator do present a risk, if intercepted by an attacker, in terms of the disruption of the model parameters themselves. This risk can be reduced if the concept of ensemble learning [51] is used, whereby different ML models are ensembled locally at the plants for usage.

Consider the model shown in Fig. 8.7 for illustration. Multiple models are trained for the prediction of one specific attack. The additional security enhancement is that different socket connections are used for parsing the model parameters. There can be two approaches to this model involving the combined use of ensemble and the FL approach. The first one consists of obtaining a local ensemble model at each plant and having the model parameters of the ensemble models parsed until the final aggregated model is obtained at the EDGE, which is then sent over to the respective plants. However, the same risk as the previous model prevails with this approach. If a cyber-attacker manages to access the model parameters of the ensemble model and modifies them, then the whole predictive model will collapse.

Thus, a second approach can be employed to increase security further. The parameters of the individual models are exchanged with the EDGE over different socket connections. Once the final model parameters are obtained at the EDGE and transferred to all the plants, a local ensemble with all the models is mounted at the plants. In the advent that the parameters of one model have been intercepted and tampered with by a cyber-attacker, the other models would compensate for the malfunction of the tampered model and help detect it after several prediction parses. This hybrid approach of using ensemble learning with FL brings about an additional security layer and a robustness feature of the local aggregated models.

Despite the increased security and robustness features that can be inherently obtained with the proposed methodology and mechanism, there is still the fact that the socket connection remains open during the whole FL process. One possible

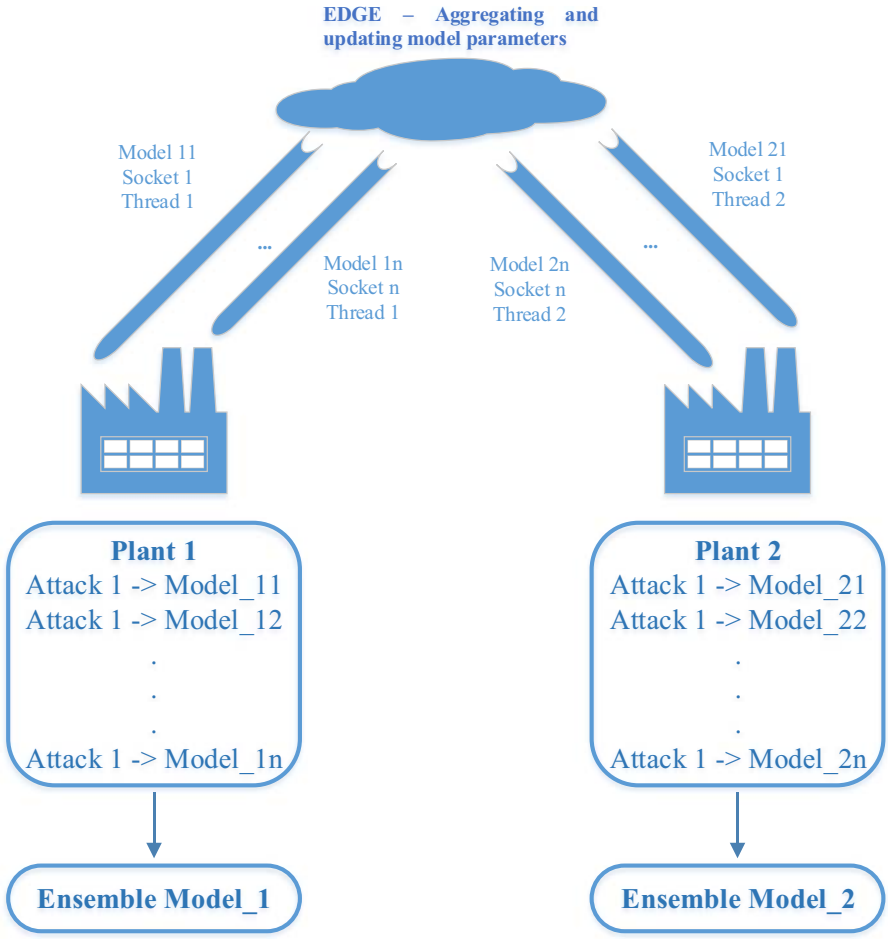


Figure 8.7 Hybrid model with federated learning and ensemble learning.

proposal would be to have an intelligent mechanism that would open the socket connection only when model parameters need to be exchanged between the plants and EDGE. Furthermore, a different socket connection could be used each time the exchange process needs to be carried out. In order to avoid complete randomness in the establishment of socket connections, a pool of TCP ports could be selected to enable intelligent selection and reuse. Additional security could be included by using secure sockets such that a secure link is established for the parameters' exchange. Further encryption mechanisms can also be incorporated at the parameters' level and have distinct cryptographic schemes associated with each plant.

The proposed layers of security would be adding complexity to the whole system. Still, the burden on the communication link is, to a very large extent, lesser

than having voluminous data transfer to a centralized location. The idea is to add to the security level already achieved when using FL. Even if an attacker manages to get hold of the model parameters after decryption of one of the models, the latter will still be required to overcome the different encryptions of the other models. Furthermore, even if the attacker alters the model parameters managed to be decrypted, the usage of the local ensemble model would be in a position to detect and handle that situation effectively.

Additional security layers can be incorporated by leveraging blockchain technology [52,53] to reinforce the defense systems against malicious cyberattacks in the realm of FL. The blockchain architecture involves the exchange and verification of local learning model updates. More specifically, the local/global model parameter weights can be saved on a blockchain ledger to ensure the security of the respective models. Moreover, the use of differential privacy mechanisms with FL is being extensively investigated to tackle data privacy concerns [54,55]. More robust hybrid data privacy and anonymization algorithms [56], involving differential privacy, k-anonymity, k-map, and *l*-diversity, could also be investigated.

Modern energy grids consist of numerous renewable plants interconnected with each other. This setup comes with a high level of individual uncertainties to the global system. However, the FL mechanism evaluated in this chapter is suitable for modern energy grids in the sense that a security mechanism is put in place to protect the ML/ensemble models used for detecting these uncertainties. In addition, the FL model put in place has the ability to incorporate the newly detected and learned uncertainties locally and further aggregate it in the global model.

8.7 Conclusion

CEIs are rapidly adopting a combination of IoT architectures and intelligent systems for data acquisition and actionable insights. Increasing the smartness of legacy systems entails the opening up of communication links, thereby making CEIs more prone to cyberattacks. Additionally, ML is being extensively investigated and deployed in CEIs for predictive analytics, and one approach that is gaining significant ground is FL. FL can offer privacy-enhanced solutions for smart grid operations. It avoids the transmission to the cloud and possible leakage of information, such as energy preferences, power traces, and addresses of individual households or companies. In this work, a review of cyberattacks in smart grids has been presented together with FL and its challenges. A system model of FL in CEIs for detecting cyberattacks has been simulated, and the corresponding results are presented. As such, the main achievement of this chapter lies in the presentation of a simulated framework of a FL environment related to CEIs. Another achievement and contribution of this chapter deals with the assessment of the potential security threats in the simulated architecture for FL and the insights provided toward possible countermeasures that could be implemented to obtain a more robust system and move closer to the possibility of standardization.

References

[1] E. Egozcue, D.H. Rodríguez, J.A. Ortiz, V.F. Villar, L. Tarrafeta, "Smart grid security," 25 April 2012. [Online]. Available: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/smart-grids/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf. (accessed 12.05.21).

[2] M.Z. Gunduz, R. Das, "Analysis of cyber-attacks on smart grid applications," in: International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 2018.

[3] S. Gorman, "Electricity grid in U.S. penetrated by spies," The Wall Street Journal, 8 April 2009. [Online]. Available: https://www.wsj.com/articles/SB123914805204099085. (accessed 12.05.21).

[4] R. Masood, "Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives," 15 August 2016. [Online]. Available: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/GW-CSPRI-2016-03 + MASOOD + Rahat + Nuclear + Power + Plant + Cybersecurity.pdf. (accessed 12.05.21).

[5] Cybersecurity and Infrastructure Security Agency, "Cyber-attack against Ukrainian critical infrastructure," 23 August 2018. [Online]. Available: https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01. (accessed 12.05.21).

[6] H.J. Mai, "NERC finds first remote hacker interference on US grid from cyberattack," Utility dive, 9 September 2019. [Online]. Available: https://www.utilitydive.com/news/nerc-finds-first-remote-hacker-interference-on-us-grid-from-cyberattack/562478/. (accessed 13.05.21).

[7] B. Sussman, "Revealed: details of 'first of its kind' disruptive power grid attack," Secure World, 8 October 2019. [Online]. Available: https://www.secureworldexpo.com/industry-news/first-u.s.-power-grid-attack-details. (accessed 9.05.21).

[8] R. Borgaonkar, T.I. Anne, D.M. Zenebe, J.M. Gilje, Improving smart grid security through 5G enabled IoT and edge computing, Concurrency Computation: Pract. Experience 33 (18) (2021) e6466.

[9] N.H. Motlagh, M. Mohammadrezaei, J. Hunt, B. Zakeri, Internet of Things (IoT) and the energy sector, Energies 13 (2) (2020) 494.

[10] C. Bormann, "CoAP - RFC 7252 Constrained application protocol," Technology Center for Computer Science and Information Technology, 2014−2016. (2016) [Online]. Available: https://coap.technology/. (accessed 29.04.22).

[11] Y. Kabalci, E. Kabalci, S. Padmanaban, J.B. Holm-Nielsen, F. Blaabjerg, Internet of things applications as energy internet in smart grids and smart environments, Electronics 8 (9) (2019) 972.

[12] M.M. Mahmoud, N. Saputro, P.K. Akula, K. Akkaya, Privacy-preserving power injection over a hybrid AMI/LTE smart grid network, IEEE Internet Things J. 4 (4) (2016) 870−880.

[13] T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, Cybersecurity in power grids: challenges and opportunities, Sensors 21 (18) (2021) 6225.

[14] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2) (2019).

[15] S. Niknam, H.S. Dhillon, J.H. Reed, Federated learning for wireless communications: motivation, opportunities and challenges, IEEE Commun. Mag. 58 (6) (2020) 46−51.

[16] L. Li, Y. Fan, M. Tse, K.-Y. Lin, A review of applications in federated learning, Computers & Ind. Eng. 149 (2020).

[17] T. Li, A.K. Sahu, A. Talwalkar, V. Smith, Federated learning: challenges, methods, and future directions, IEEE Signal. Process. Mag. 37 (3) (2020) 50−60.
[18] V. Mothukuri, R.M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, Future Gener. Computer Syst. 115 (2021) (2021) 619−640.
[19] J. Feng, Q.-Z. Cai, Z.-H. Zhou, "Learning to confuse: generating training time adversarial data with auto-encoder," arXiv, 22 May 2019.
[20] L. Muñoz-González, B. Biggio, A. Demontis, A. Paudice, V. Wongrassamee, E.C. Lupu, et al., "Towards poisoning of deep learning algorithms with," Proceedings of the 10th ACM Workshop, pp. 27−38, 2017.
[21] B. Biggio, B. Nelson, P. Laskov, "Poisoning attacks against support vector," arXiv, pp. 1−8, 25 March 2013.
[22] D. Cao, S. Chang, Z. Lin, G. Liu, D. Sun, "Understanding distributed poisoning attack in federated learning," in: IEEE 25th International Conference on Parallel and Distributed Systems, 2019.
[23] G.F. Cretu-Ciocarlie, A. Stavrou, M.F. Locasto, S.J. Stolfo, A.D. Keromytis, "Casting out demons: Sanitizing training data for anomaly sensors," in: IEEE Symposium on Security and Privacy, 2008.
[24] E. Bagdasaryan, A. Veit, Y. Hua, D. Estrin, V. Shmatikov, "How to backdoor federated learning," in: International Conference on Artificial Intelligence, 2020.
[25] A.N. Bhagoji, S. Chakraborty, P. Mittal, S. Calo, "Analyzing federated learning through an adversarial lens," in: International Conference on Machine Learning, 2019.
[26] M. Fang, X. Cao, J. Jia, N.Z. Gong, "Local model poisoning attacks to Byzantine-Robust Federated Learning," in: Usenix Security Symposium, 2019.
[27] A. Shafahi, W.R. Huang, M. Huang, O. Suciu, C. Studer, T. Dumitras, et al., "Poison frogs! targeted clean-label poisoning attacks on neural networks," in: Proceedings of the 32nd International Conference on Neural Information Processing Systems, 2018.
[28] M. Nasr, R. Shokri, A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in: IEEE Symposium on Security and Privacy, 2019.
[29] Z. Sun, P. Kairouz, A.T. Suresh, H.B. McMahan, "Can you really backdoor federated learning?," in: 2nd International Workshop on Federated Learning for Data Privacy and Confidentiality at NeurIPS, 2019.
[30] K. Liu, B. Dolan-Gavitt, S. Garg, "Fine-pruning: defending against backdooring attacks on deep neural networks," in: International Symposium on Research in Attacks, Intrusions, and Defenses, 2018.
[31] Y. Jiang, S. Wang, B.J. Ko, W.-H. Lee, L. Tassiulas, "Model pruning enables efficient federated learning on edge devices," arXiv, 23, 2020, 2019.
[32] B. Hitaj, G. Ateniese, F. Perez-Cruz, "Deep models under the GAN: information leakage from collaborative deep learning," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017.
[33] Y. Zhao, J. Chen, J. Zhang, D. Wu, J. Teng, S. Yu, PDGAN: a novel poisoning defense method in federated learning using generative adversarial network, Algorithms and Architectures for Parallel Processing, Springer, 2020.
[34] S. Li, Y. Cheng, W. Wang, Y. Liu, T. Chen, "Learning to detect malicious clients for robust federated learning," arXiv, 1 February 2020.
[35] X. Cao, J. Jia, N.Z. Gong, "Provably secure federated learning against malicious clients," arXiv, 3 February 2021.

[36] S. Shen, S. Tople, P. Saxena, "Auror: defending against poisoning attacks in collaborative deep learning systems," in: Proceedings of the 32nd Annual Conference on Computer Security Applications, 2016.
[37] C. Fung, C.J.M. Yoon, I. Beschastnikh, "Mitigating sybils in federated learning poisoning," arXiv, 15 July 2020.
[38] J. Konecny, H. Brendan McMahan, F.X. Yu, A.T. Suresh, D. Bacon, "Federated learning: strategies for improving communication efficiency," arXiv, 30 October 2017.
[39] H.B. McMahan, E. Moore, D. Ramage, S. Hampson, B.A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in: Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, 2017.
[40] L. Wang, W. Wang, B. Li, "CMFL: mitigating communication overhead for federated learning," in: IEEE 39th International Conference on Distributed Computing Systems, 2018.
[41] X. Yao, C. Huang, L. Sun, "Two-stream federated learning: reduce the communication costs," in: IEEE Visual Communications and Image Processing, VCIP, 2018.
[42] D. Li, J. Wang, "FedMD: heterogenous federated learning via model distillation," arXiv, 8 October 2019.
[43] V. Smith, C.-K. Chiang, M. Sanjabi, A. Talwalkar, "Federated multi-task learning," in: 31st Conference on Neural Information Processing Systems, Long Beach, CA, USA, 2017.
[44] J. Lin, M. Du, J. Liu, "Free-riders in federated learning: attacks and defenses," arXiv, 28 November 2019.
[45] B. Zong, Q. Song, M.R. Min, W. Cheng, C. Lumezanu, D. Cho, et al., "Deep autoencoding Gaussian mixture model for unsupervised anomaly detection," in: International Conference on Learning Representations, 2018.
[46] R. Colbaugh, K. Glass, "Moving target defense for adaptive adversaries," in: IEEE International Conference on Intelligence and Security Informatics, 2013.
[47] V. Mallawaarachchi, "Introduction to genetic algorithms—including example code," towards data science, 8 July 2017. [Online]. Available: https://towardsdatascience.com/introduction-to-genetic-algorithms-including-example-code-e396e98d8bf3#:~:text=A%20genetic%20algorithm%20is%20a,offspring%20of%20the%20next%20generation. (accessed 18.04.21).
[48] H. Shin, W. Lee, J. Yun, H. Kim, "HAI 1.0: HIL-based Augmented ICS Security Dataset," in 13th USENIX Workshop on Cyber Security Experimentation and Test, Santa Clara, CA, 2020.
[49] S. Choi, J.H. Yun, S.K. Kim, A comparison of ICS datasets for security research based on attack paths, Critical Information Infrastructures Security, Springer, 2019.
[50] ICS (Industrial Control System) Security Dataset, "ICS (Industrial Control System) Security Dataset," Github, 2020. [Online]. Available: https://github.com/icsdataset/hai. (accessed 17.04.21).
[51] B. Dickson, "What is ensemble learning?," TechTalks, 12 November 2020. [Online]. Available: https://bdtechtalks.com/2020/11/12/what-is-ensemble-learning/. (accessed 18.04.21).
[52] H. Kim, J. Park, M. Bennis, S. Kim, Blockchained on-device federated, IEEE Commun. Lett. 24 (6) (2020) 1279−1283.
[53] U. Majeed, C.S. Hong, "Federated learning via MEC-enabled blockchain network," in: 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019.

[54] K. Wei, J. Li, M. Ding, C. Ma, H.H. Yang, F. Farokhi, et al., Federated Learning With Differential Privacy: Algorithms and Performance Analysis, IEEE Trans. Inf. Forensics Security 15 (2020) 3454−3469.

[55] N. Rodríguez-Barroso, G. Stipcich, D. Jiménez-López, J.A. Ruiz-Millán, E. Martínez-Cámara, G. González-Seco, et al., Federated learning and differential privacy: software tools analysis, the Sherpa.ai FL framework and methodological guidelines for preserving data privacy, Inf. Fusion. 64 (2020) 270−292.

[56] Y.N. Fakeeroodeen, Y. Beeharry, Hybrid data privacy and anonymization algorithms for smart health applications, SN Computer Sci. 2 (126) (2021).

This page intentionally left blank

A lightweight string-matching technique for secure communication within IoT energy systems technology

9

Mohammad Equebal Hussain[1], *Mukesh Kumar Gupta*[1] *and Rashid Hussain*[2]
[1]Suresh Gyan Vihar University, Jaipur, Rajasthan, India, [2]Moti Babu Institute of Technology, Forbesgunj, Bihar, India

Chapter Outline

9.1 Introduction

Because of the rapid increase in internet-based technologies, cloud computing provides a large-scale and powerful computing infrastructure for various applications. IoT devices generate large-scale data for real-time critical applications. Those data need to be preprocessed before transmitting onto the cloud for storage and further processing. The cloud computing platform offers big data storage, as well as large-scale processing services. The cloud service can be used to integrate the complete life cycle of data collection, transmission, processing, storage, and analytics; however, the above-mentioned infrastructure also suffers from security and privacy threats due to shared and multitenancy features supported by cloud computing [1]. Many issues have already been addressed and continued. Continuous enhancement needs more investigation of related issues in this field for the wide deployment of

IoT Enabled Multi-Energy Systems. DOI: https://doi.org/10.1016/B978-0-323-95421-1.00007-0

applications on the cloud. Since the semantics of data keeps on changing, security systems also need a continuous understanding of the data pattern, user, system, and how event interact with the data in order to protect it. Effective research is required for more scalable detection and prevention techniques in the cloud computing environment. In this paper, we will propose an efficient real-time string-matching technique, which helps in monitoring the device from malicious activities against various attacks varying from network packet monitoring to sensitive and confidential information detection and prevention.

For all our proofs and implementations, we have used the multifast library and tool [2] implemented in C programming language efficient tool for mass string search solution via Aho−Corasick (AC) algorithm. Along with multifast, we also used regular expression validation using the PCRE2-based regex101 library [3]. All the state diagram for finite state machine is drawn using JFLAP [4]. All the diagrams are constructed using draw.io [5]

9.2 Background

In this section, we will discuss several related algorithms, such as the Knuth−Morris−Pratt algorithm (KMP) and AC string-matching techniques, and their possible applications in cloud security using a virtual wireless sensor network. These techniques are very useful for maintaining real-time cloud-scale security and confidentiality for sensitive content to comply with data privacy laws and regulations like HIPAA policy. The current traditional policy-based approach, combined with dictionary and regular expression, still exists and is valid. This approach is based on string matching of related keywords maintained in a well-defined dictionary. The demand for the detection of sensitive information from its semantic contextual information through machine learning, AI, and deep learning techniques are, however, increasing. The data loss prevention (DLP) strategy ensures regulatory compliance, as well as the security of personnel health information, personnel identifiable information, and intellectual property (IP), during the transmission [6] from the private cloud to the public cloud when such risks are high. In Ref. [6], context-aware detection methods claim a better performance over the existing dictionary-based methods.

9.2.1 *Knuth−Morris−Pratt algorithm*

KMP [7] is one of the well-known string search algorithms improving over the naive string search algorithm where every character input search string n is compared with each character in the input text m. The KMP algorithm approach is to create a failure function for each character in m, defining the number of characters, which can be skipped during a failed partial match in m. This technique results in no backing up while iterating “m”, that is, no character in “m” will, in the worst case, be compared more than once, and therefore, result in a linear time O(|n|)

complexity with respect to the size of "n". There will be an added time complexity when constructing the failure function, which also has a linear time complexity with respect to the size of the search string m, resulting in overall time complexity of Θsize (m) + size(n) [8].

9.2.2 Aho−Corasick algorithm

According to AC [9], string search algorithm based on a finite state machine (FSM) constructed from a list of keywords K. The main goal of this algorithm is to locate all occurrences of K in a text string. Any Aho−Corasick finite state machine (AC-FSM) is defined using six tuples [10] defined in Eq. 9.1.

$$\text{AC-FSM} = \{Q, \sum, \delta, \Delta, q_0, F\} \tag{9.1}$$

where Q is a set of states, $\sum$ is a set of input characters, δ is the goto function defined in Eq. 9.2, Δ is a set of success and failure functions defined in Eqs. 9.3 and 9.4, respectively. $q_0 \in Q$ is initial state, $F \subseteq Q$ is a set of the final state.

$$\text{Transition between the state goto(q, c)}: Q \times \sum \rightarrow Q \tag{9.2}$$

$$\text{Represents a pattern match success(q)}: Q \rightarrow F \tag{9.3}$$

$$\text{If c is not defined in go to function failure(q)}: Q \rightarrow Q^* \tag{9.4}$$

The fail function, that is, failure(q), is the state transition from state q_i to state q_j when no transition is defined in the goto function for the current input character. Similarly, the success function, that is, success (q), represents a successful match from list K. The finite state machine [8] is represented in Fig. 9.1 based on the TRIE data structure. AC goto() for keywords K = {'/usr/lib, '/usr/src', '/usr/bin'} is represented in Table 9.1.

The complexity of constructing state machine for the $|K|$ number of keywords is $O(|K|.L)$ where L is the average length of the keyword. Each transition takes constant time and the time complexity to process an input string of length n is $O(n + max(K))$ [8].

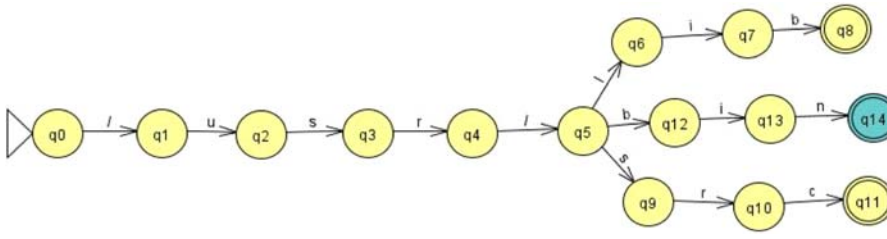


Figure 9.1 Aho−Corasick goto function.

Table 9.1 Success function.

State (q)	Success(q)
q_8	/usr/lib
q_{11}	/usr/bin
q_{14}	/usr/src

9.2.3 Data loss prevention in cloud service

In the era of cloud computing, DLP has become an important security strategy. It helps in protecting sensitive information from accidental loss of data outside of the trust zone. DLP service contains a set of policies and tools that are meant to prevent data leakage due to intentional or unintentional misuse. This equally applies to all states of data, that is, data at rest, data in motion, and data in use. In public and hybrid clouds, there exist many potential risks that need mitigation to ensure optimal utilization of service. One of the major risks is maintaining the security and confidentiality of sensitive information. Real-time detection of security content in the cloud is a critical step to preventing data loss, as well as complying with laws and regulations. For proactive early detection of sensitive data in order to govern, manage, protect, and use in the cloud environment [6], we proposed a system that could detect sensitive content using a dictionary and policy-based approach with the help of the modified AC technique. The main goal of DLP on the cloud is to ensure that, out of many cloud applications or managed and unmanaged app instances, try to find, protect and classify data used by applications, as well as data movement between SaaS cloud applications, IaaS cloud service, email, and the web. In this paper, we will propose the design of vWSN to either allow or block using policy enforcement to restrict activities such as downloading and copying. It is also a key driver mechanism to assure regulatory compliance and IP protection.

9.3 Literature review

Data protection is the most important security issue when it comes to the transfer of an organization's data to a remote machine, especially a hybrid or public cloud. Many techniques have already been proposed, but there are a lot of challenges. Some of the popular security techniques are secure socket layer, encryption, multitenancy, access control list, etc. cloud computing provides fast and cost-effective solutions using shared storage and computing resource.

9.4 Proposed architecture and design

The proposed design is based on a content-aware DLP technique using exact data match. It is a content-based data modeling technique where sensitive information

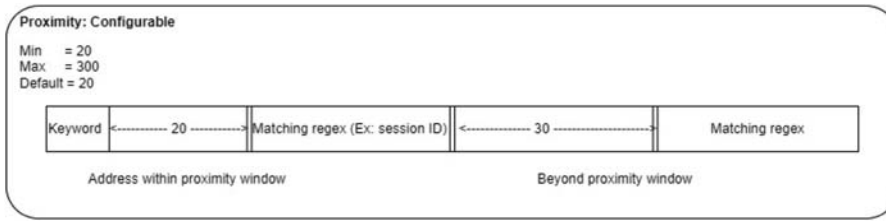


Figure 9.2 Pattern consists primary and supporting elements and proximity.

follows a certain pattern, which can be queried using regular expression. The data can be classified into pattern, keyword, confidence level, and proximity [11]. The confidence level can be further divided into high, medium, and low. Sensitive information within the document is a combination of primary and supporting element (as indicated in Fig. 9.2). Proximity is the distance between policy-defined pairs of words. If the words are within the range, then a match is triggered.

The proposed design on which thread pool consists of a group of threads to support multitenant. Each agent is assigned a free thread from the thread pool, which is responsible for processing the input streams through the AC driver program, which is a combination of a multifast string processing engine, dictionary, terms, and regular expression.

In a SaaS (software as a service) model, the above design can be easily integrated through REST API-based communication protocol to implement CRUD (create, read, update, and delete) operations based on the sensitivity of information contained in the document. The request is sent from the cloud storage service (SaaS) layer using REST API call to the DLP server to inspect files in real time for possible action. The action could allow, quarantine, or block the data that violates the regulation. It can be used for on-demand detection of files.

9.5 Result, discussion, and findings

The comparative analysis is presented along with a graph for different input file sizes, percentage of data match, and run time on a virtual machine.

Table 9.2 shows the experimental value, which is done on the Linux platform on a virtual system having 8-Gb RAM and 8-core processor intel core i9 2.3 GHz. The result is for policies having a combined dictionary and regex-based search (as indicated in Fig. 9.3) using the proposed AC model.

The final step is to match the content with the configured rule. Each rule is matched against the payload. The payload is processed through the AC state machine to determine if any of the rule matches. If the specified content is found, then a user-defined action is performed.

Table 9.2 Performance test result for multiple policies for varying sizes.

File size (kb/Mb/Gb)	Run time (ms) (no match)	25%–30% match	50%–60% match	75%–80% match	100% match
10 kb	1286	1275	1310	1289	1293
100 kb	1287	1357	1451	1525	1632
1 Mb	1327	1850	2127	2440	2530
50 Mb	3371	15,932	15,783	17,515	17,900
100 Mb	5380	15,839	15,767	17,954	17,698
1 Gb	42,858	15,656	16,000	17,634	17,664

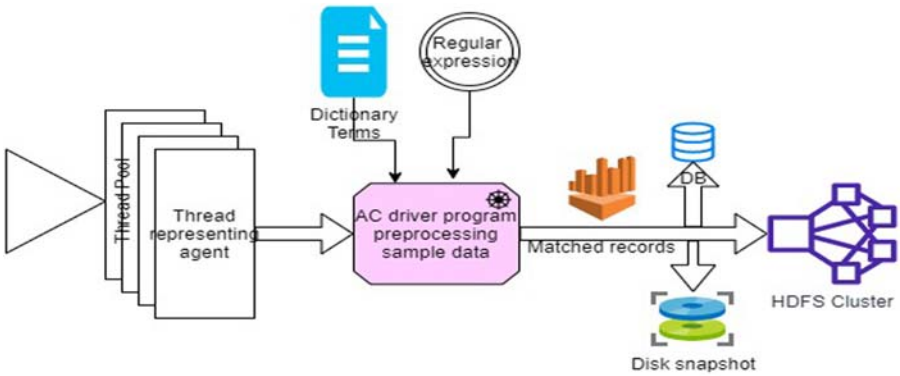


Figure 9.3 Aho–Corasick-based policy engine.

9.5.1 Performance test result

In the below graph (as indicated in Fig. 9.4) is shown the percentage of record matches on the x-axis, ranging from (0, 100, 25) in the sample data that varies from 10 kb to 1 Gb, whereas the y-axis represents the run time in ms. It is observed that when a sample doesn't match, then the time taken to run the policies is proportional to the sample size, which is also the same as the naïve method, which always remains proportional to file size. The algorithm performs well when the sample contains matching data.

The graph in Fig. 9.5, is the result where the x-axis represents file size, and the running time (ms) on the y-axis.

9.5.2 Comparative analysis of Aho–Corasick versus Knuth–Morris–Pratt

Fig. 9.5 shows average run time for pattern match using AC and KMP algorithm. Different experiments [8] show that performance of the AC algorithm is much better after a threshold point.

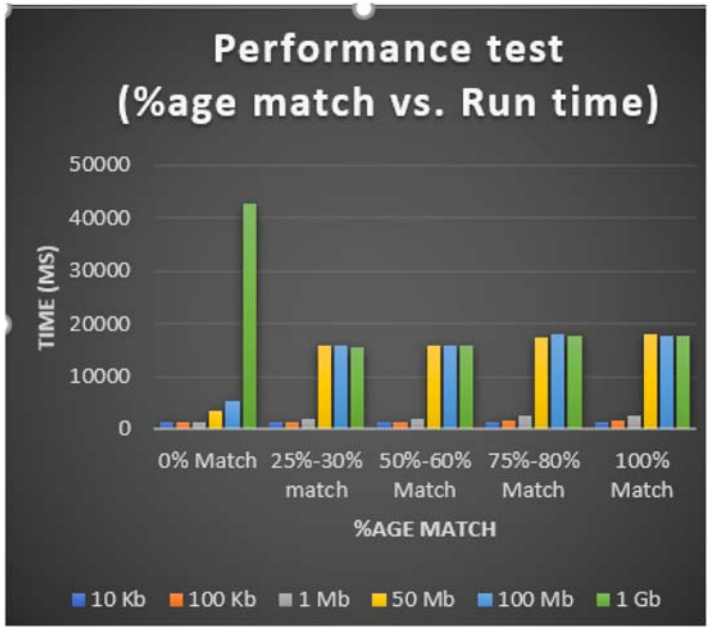


Figure 9.4 Percentage match versus run time (ms).

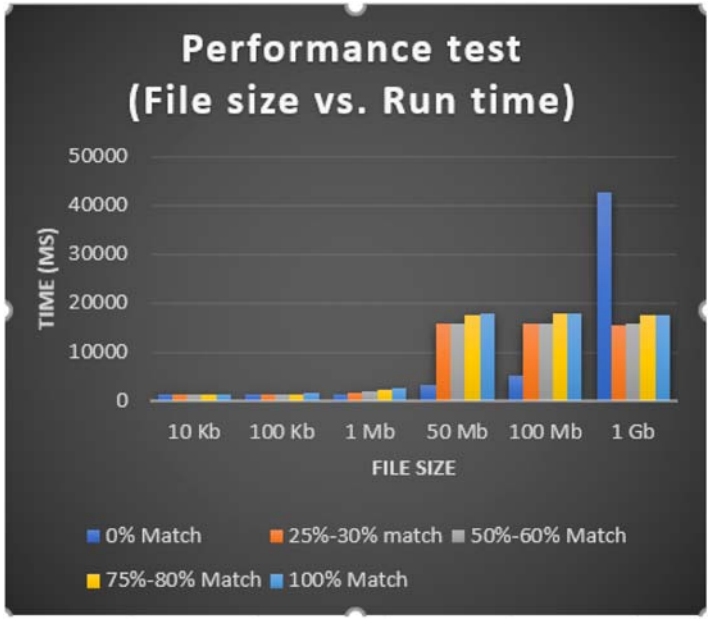


Figure 9.5 File size versus run time (ms).

9.6 Conclusion

In this paper, we introduced a model using a dictionary, regular expression combined with AC string-matching technique for detecting sensitive content in the public and hybrid cloud model. It also leverages contextual semantic information to some extent. The proposed DLP system can detect sensitive content at various granularity levels within the document and respond immediately to any event or behavior that violates data sensitivity compliance. We also demonstrate that for various synthetic data on the proposed model and methods, the system is capable enough to mitigate future threats that could help in applying strong security and integrity of their hybrid cloud by taking appropriate preventative measures.

Acknowledgments

I would like to thank Dr. Mukesh Kumar Gupta and Dr. Rashid Hussain for their encouragement and support during the research.

Thanks for the reviewer's comments and suggestions, which are addressed in the best possible way.

References

[1] X. Zhang, Y. Yuan, Z. Zhou, S. Li, L. Qi, D. Puthal, Intrusion detection and prevention in cloud, fog, and internet of things, Hindawi (2019).
[2] Online, Available from: http://sourceforge.net/projects/multifast/files/multifastv0.6.2/multifast-v0.6.2.tar.gz.
[3] Available from: https://regex101.com/.
[4] Online, Available from: "JFLAP." https://www.jflap.org.
[5] Software for making diagrams and charts. Online, Available from: https://app.diagrams.net/.
[6] Y.J. Ong, M. Qiao, R. Routray, R. Raphael, "Context-aware data loss prevention for cloud storage services," in: 2017 IEEE 10th International Conference on Cloud Computing (CLOUD), 2017, pp. 399−406.
[7] D.E. Knuth, J. Morris, H. James, V.R. Pratt, Fast pattern matching in strings, SIAM J. Comput. 6 (2) (1977) 323−350.
[8] C. Nykvist, M. Larsson, A.H. Sodhro, A. Gurtov, A lightweight portable intrusion detection communication system for auditing applications, Int. J. Commun. Syst. 33 (7) (2020) e4327.
[9] A.V. Aho, M.J. Corasick, Efficient string matching: an aid to bibliographic search, Commun. ACM 18 (6) (1975) 333−340.
[10] M.E. Hussain, R. Hussain, "Real time Aho-Corasick Implementation of String Matching technique suitable for smart IOT," in: 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1−6, doi: 10.1109/SMARTGENCON51891.2021.9645846.
[11] "Learn about sensitive information types - Microsoft 365 Compliance | Microsoft Docs." https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about?view = o365-worldwide (accessed Nov. 21, 2021).

Index

Note: Page numbers followed by "*f*" and "*t*" refer to figures and tables, respectively.

IoT Enabled Multi-Energy Systems

From Isolated Energy Grids to Modern Interconnected Networks

Reviews the transition from isolated energy grids to modern interconnected networks by providing a formal theory and IoT-based practical solutions for multi-energy systems

IoT Enabled Multi-Energy Systems proposes practical solutions for the management and control of energy interactions throughout the interconnected energy infrastructures of the future multi-energy grid. It discusses a panorama of modeling, planning, and optimization considerations for IoT technologies and their applications across grid modernization and the coordinated operation of multivector energy grids. The work is suitable for energy, power, mechanical, chemical, process, and environmental engineers and is highly relevant for researchers and postgraduate students who work on energy systems.

Sections address core theoretical underpinnings, significant challenges and opportunities, and supporting IoT-based developed expert systems, working to identify how artificial intelligence (AI) can empower IoT technologies to sustainably develop fully renewable modern multicarrier energy networks. It also provides proven methodologies, establishes worked solutions, and develops a holistic framework for proposing IoT-based solutions for intelligently modernizing future multivector energy grids. Motivations and obstacles of the deployment of advanced IoT technologies are discussed in detail.

Contributors address AI technology and its applications in developing IoT-based technologies; cloud-based intelligent energy management schemes; data science and multi-energy big data analysis; machine learning and deep learning techniques in multi-energy systems; cyber-physical multi-energy systems; blockchain technology; reliable and sustainable development of the modern energy networks; design, integration, and operation of a high/full level of renewable energy resources; optimal energy management systems; optimization of hybrid energy systems' utilization; grid-edge technologies; and hybrid energy components.

- Reviews core applications of IoT technologies in grid modernization of multi-energy networks
- Develops practical solutions for optimal integration of renewable energy resources in modern multivector energy networks
- Analyzes the reliable integration, sustainable operation, and accurate planning of multicarrier energy grids in highly penetrated stochastic energy resources

About the editors

Mohammadreza Daneshvar is a researcher with the Department of Electrical and Computer Engineering at the University of Tabriz. He is the author of more than 40 journal and conference papers in the field of energy and electrical engineering. He also is the author and editor of six books with Springer, Elsevier, and Wiley-IEEE Press. He serves as an active reviewer and ranked among the top 1% of reviewers in engineering and cross-field.

Behnam Mohammadi-Ivatloo, PhD, is currently a full professor of electrical and computer engineering at the University of Tabriz. He is formerly a research associate at the University of Calgary. He obtained his MSc and PhD degrees in electrical engineering from the Sharif University of Technology. He is the author and editor of more than 19 books in the field of energy and electrical engineering.

Kazem Zare, PhD, received his BSc and MSc degrees in electrical engineering from the University of Tabriz and PhD degree from the Tarbiat Modares University, Tehran, Iran. Currently, he is a professor in the Faculty of Electrical and Computer Engineering at the University of Tabriz. He is the author and editor of six books in the publication process with Springer, Elsevier, and Wiley-IEEE Press.

Amjad Anvari-Moghaddam, PhD, is currently an associate professor and the leader of the Intelligent Energy Systems and Flexible Markets (iGRIDS) research group at AAU Energy, Aalborg University, where he is also the coordinator for the Integrated Energy Systems Laboratory. He has published more than 270 technical articles, 8 books, and 16 book chapters in the field of planning, control, and operation management of energy systems.

ACADEMIC PRESS

An imprint of Elsevier

elsevier.com/books-and-journals

ISBN 978-0-323-95421-1