# An Overview of Cyber-Security Issues in Smart Grid


**Mayank Srivastava**

**Abstract** A smart grid is an updated version of the traditional electrical grid that uses Information and Communication Technology (ICT) in an automated fashion for the production and distribution of electricity. Several attributes like efficiency, sustainability, and reliability are improved in the smart grid as compared to the traditional grid. Smart grid gives significant benefits for the entire community, but their dependence on computer networks make them vulnerable to various kinds of malicious attacks. This article focuses on identifying the various cyber-security issues of different areas of the smart grid which are prone to vulnerabilities. Finally, the possible solutions for resolving the cyber-security issues in the identified areas for making the smart grid more secure were analyzed.

**Keywords** Smart grid · ICT · Smart devices · Cyber-security · Vulnerability

## 1 Introduction

Smart grid technology offers many benefits to the entire society [1]. However, the integration of computer networks into the smart grid makes society vulnerable to different types of malicious attacks. Also, such integration makes the way for the privacy issues of the customer. The ICT is the basis of the underlying smart grid infrastructure, which is required for the successful operation of the smart grid. Henceforth, it becomes necessary to address the security issues of ICT in this domain. Finally, one can say that it is important to address the cybersecurity issues in various phases of the smart grid [2].

Besides this, the unintentional compromises of the network infrastructure due to user-oriented errors, apparatus failures, and natural blows also need to be considered. Securing the entire facility of the smart grid is a daunting task [3]. The vulnerabilities of the existing technology infrastructure must first be identified and analyzed, before applying the management process to mitigating them. But there are certain barriers

M. Srivastava (✉)
Department of CEA, GLA University, Mathura 281406, UP, India
e-mail: mayank.srivastava@gla.ac.in



A. Pasumpon Pandian et al. (eds.), *Computer Networks, Big Data and IoT*, Lecture Notes on Data Engineering and Communications Technologies 66,
https://doi.org/10.1007/978-981-16-0965-7_49

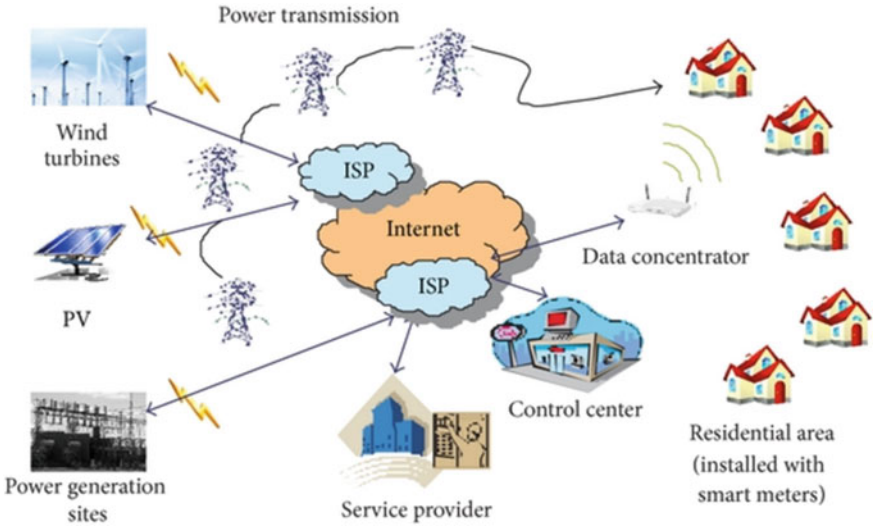


**Fig. 1** Smart grid architecture [5]

such as organizational issues, lack of technical skills, and awareness concerns that prevent us to achieve this objective. [4].

A smart grid basically incorporates a computer network with the existing grid infrastructure to analyze and distribute data related to energy consumption. In the smart grid, the energy producers and energy consumers interact intelligently which eventually serves the purpose of saving a lot of energy. In Fig. 1, the different forms of energy generation schemes like wind turbines, photo-voltaic (PV), and power generation sites are used for power generation. The generated power is distributed to various categories of customers. The figure also shows the interconnection of various nodes across the entire transmission network of the smart grid. The various network components used in the infrastructure are data concentrator, control center, Internet Service Provider (ISP), and various sensors. The sensors are used to give accurate information about different aspects of smart grid architecture.

## 2 Review of Literature

Different researchers are working on various domains of the smart grid. Some of the major contributions of the research done in this area are as follows.

Chebbo [3] focuses on the importance of smart technologies, smart vision, smart processes, and finally smart stakeholders for energy innovation. Tuballa et al. [4] present an outline of the associated technologies of the smart grid. The paper also mentions the importance of the latest technologies in influencing the existing grid. Mrabet et al. [5] provide a deep understanding of the security vulnerabilities and their

possible solutions. The paper gives a cyber-security strategy to deal with various kinds of cyber-attacks. Wang et al. [6] put a thought on the hybrid structure of the computer networks that connect the energy providers and consumers in a smart grid. The author then emphasizes the challenging problems of network reliability and security. Bigerna et al. [7] perform the literature review about the social costs affecting the development of the smart grid. The paper finally presents the opportunities and challenges in the business, applications, policy, and security issues of the smart grid.

Kappagantu et al. [8] specify that the three main objectives of cybersecurity that need to be addressed are availability, integrity, and confidentiality. It also emphasized on multilayer structure of the smart grid, where each layer is having specific security concerns. Finally, it states that the use of advanced techniques is essential to tackle sophisticated cyber threats. Baumeister [9] proposes a study that is divided into five different smart grid security categories namely process control, communication protocol, smart meter, simulation for security analysis, and power system state estimation for achieving smart grid security. Wang et al. [10] present a comprehensive review of different cybersecurity issues for the smart grid which focuses on various vulnerabilities and solutions concerning the smart grid.

Yang et al. [11] discuss the various cyber-attacks and their possible solutions which are crucial for the expected operation of the smart grid. The paper also presented its insight on the critical aspects related to cyber-security of smart grid-like interdependency, vulnerability, etc. Pearson [12] presented a study on the use of ICT in Europe's electricity sector. The article highlights that increased reliance on ICT in the electricity sector will open up new vulnerabilities that will undermine the advantage of the smart grid. It also explains that the European Union (EU) has to mitigate these challenges to avoid a possibly expensive technical lock-in. Yan et al. [13] summarize the different cybersecurity issues and vulnerabilities related to the smart grid. It also presents a survey that focuses on the current solutions to different cybersecurity issues of smart grids.

Aillerie et al. [14] present the report which identifies significant issues in cybersecurity policy design for the International Smart Grid Action Network (ISGAN) membership. The paper discusses the smart grid architecture along with fast-changing cyber threats. The paper also proposes certain hardware designs for improving the security of the smart grid. Berthier et al. [15] focus on using secure protocols to prevent the network from being exploited. It also emphasizes the importance of intrusion detection system (IDS). Sou et al. [16] explore the smart grid cybersecurity problem by analyzing the false data attacks-based vulnerabilities of electric power networks. Here, the analysis of the problem is based on the constraint cardinality minimization problem. It was shown in the paper that a relaxation technique provides an exact optimal solution to the cardinality minimization problem.

## 3 State Estimation of Smart Grid

Figure 2 shows another basic infrastructure of the smart grid. It can be seen from the given figure that it includes cloud-based servers, power transmission lines, smart grid operators, and transmission lines to the industrial, commercial, and residential customers. The whole smart grid infrastructure is based on smarter networks, which are mainly used for transmission and distribution purposes [17]. The smart grid makes use of mostly new technologies to improve the transmission as compared to the traditional system. Advanced distribution automation (ADA) technologies along with advanced metering infrastructures (AMI) provides the required intelligence to the power grid infrastructure to meet out its defined expectations.

The smart grid acts intelligently to integrate distributed energy generation from different energy sources. A smart grid helps mainly in conserving energy, increasing reliability and transparency, reducing cost, and making the entire process of energy generation and distribution more efficient [18]. In a smart grid, the data between consumers and the grid operator is exchanged by using secure communication channels based on encryption. Here, the homomorphic data encryption techniques are used to provide data privacy over the cloud.

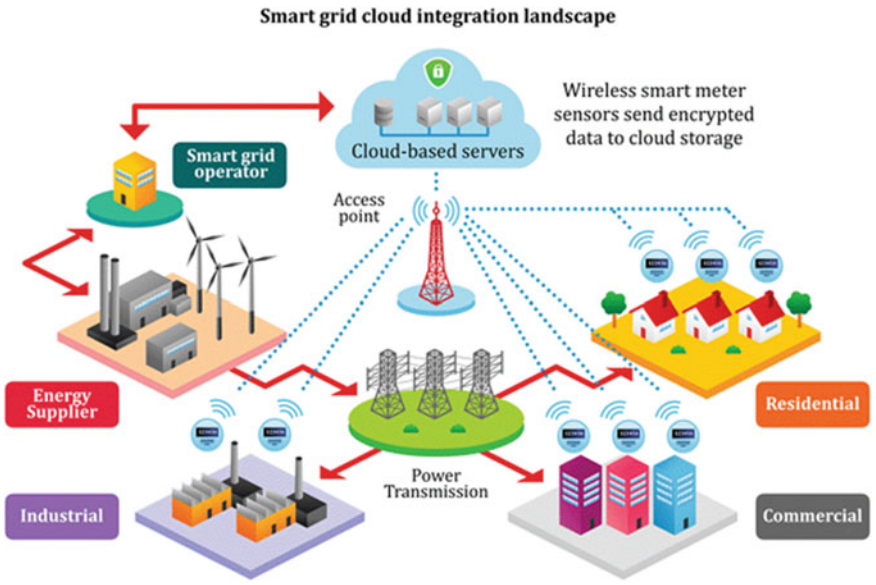


**Fig. 2** The smart grid architecture [17]

## 4 Cyber-Security Issues in Smart Grid

Smart grid infrastructure dominantly uses smart devices that are prone to vulnerabilities. As the smart grid makes heavy use of ICT, this gave the attackers a possibility to exploit the different vulnerabilities of ICT to disrupt the normal operation of the grid. A smart grid is an interconnection of heterogeneous systems, where each system may be having its own set of technologies and communication equipment. This heterogeneity, diversity, and complexity make the security of the smart grid highly difficult. The objective of this section is to highlight the major cyber-security issues of different areas of the smart grid, which is having vulnerabilities and can be exploited by the attackers to do malicious activity [19]. The various cyber-security issues in different areas are as follows:

1. **Architecture**: The weakness of the smart grid architecture can be exploited by the intruder for a possible attack. For example, vulnerabilities related to the operating system, server, etc. can be exploited to perform malfunctioning of the system.
2. **Communication protocols**: Devices can be compromised if they are communicating over an insecure line. Some of the widely used wireless protocols like Zigbee, Wimax, Wifi are also having vulnerabilities.
3. **Interfaces**: Web-based smart grid applications are subject to several vulnerabilities. The vulnerabilities related to the application can be exploited to make the system error-prone.
4. **Home area networks (HAN)**: Vulnerability can also exist in smart equipments within HAN. Network parameters of HAN can be identified to launch various network attacks.
5. **Human factor**: Social engineering techniques can be adopted by the attacker to access customer accounts and to change their settings. For example, by using phishing attacks, the attacker can get the basic details related to the customer and exploit the system.
6. **Physical security**: Physical exposure of the network components and smart devices are vulnerable to intrusion. If devices are not properly physically secured, anyone can connect to them to change the network settings or may perform any malicious activity.

There are several ICT-based smart grid components that also suffer from different cyber-security issues.

1. **Operational systems**: Meter Data Management System (MDMS), Supervisory control and data acquisition (SCADA) Systems, Utility system, etc. For example, the system may have several open ports that can be exploited by the attacker.
2. **Standard IT systems**: PCs, servers, mainframes, application server, database server, web server, etc. For example, there is a possibility that apart from port numbers generated by specific applications other port numbers can be open, which can be exploited by the attacker.

3. **Terminating devices**: Smartphones, electric vehicles, smart meters, and other mobile devices. For example, smart meters can be hacked to increase or decrease power demand.

## 5 Possible Solutions of the Cyber-Security Issues

It is evident from the previous section that the smart grid is vulnerable to different types of cyber-security issues. To deal with these vulnerabilities, prevention is considered to be the most effective strategy as compared to elimination. This section provides a possible solution to deal with various cyber-security issues mentioned in different areas of the previous section [5, 9, 13].

1. **Architecture**: It must be designed so that they can be able to handle malicious attacks like denial-of-service (DOS). The network must also be able to cope-up with the network failures oriented attacks by maintaining the automation service locally.
2. **Communication protocols**: To make communication secure, end-to-end encryption must be used. Secure wireless protocols like WPA2 can be used for securing data in wireless networks.
3. **Interfaces**: Web interfaces can be secured by following one or many of the given means: context output encoding, secure password storage, multi-factor authentication, etc. Context output encoding is a programming technique that can prevent cross-site scripting flaws.
4. **Home area networks**: Wireless communications between smart appliances and central systems should be secured by using encryption. Also, there is a need to eliminate rogue access devices to protect against interception or manipulation.
5. **Human factors**: The devices should be capable to use encryption for achieving authentication and authorization to prevent sniffing password attacks. The process of creating user-id and password should be complex to thwart any dictionary-based attacks.
6. **Physical Security**: Providing physical security of the entire network including connected devices is majorly a daunting task. However, infrastructure at the grid, sub-station, and (if possible) at the customer level must be protected by some means of physical guarding and surveillance guarding for physical security.

The smart grid's ICT components are also needed to be resolved for vulnerability so that the cyber-security issues related to them can also be prevented.

1. **Operational Systems**: The operational systems may include one or many of the components like wireless communication, data collection and management, and utility system. The means of securing each one of them is already given in the discussion above.
2. **Classic IT systems**: The IT systems especially web servers, application servers, the database server can be made more secure by resolving the vulnerabilities related to their operating systems, applications, protocols, and network. The

found vulnerabilities can be resolved by updating them through the required patch given by the solution provider.

3. **Terminating devices**: The terminating devices must be purchased from the authorized center, and their operating system and applications must be updated regularly for achieving security.

## 6 Conclusion

Smart grid technology is a recent research area in which issues of existing grid infrastructure are addressed. The smart grid is basically used to monitor various grid-oriented activities, load side preferences, and to perform real-time actions. The smart grid consists of various distributed and heterogeneous computer systems, required to integrate the various forms of energy and to deliver electricity more easily to the consumers. Despite the various advantages of the smart grid, there are multiple challenges in its implementation which include coordination and adoption of the new technology. This article focuses on identifying different cyber-security issues about the current state of a smart grid. These important issues need to be addressed to make the smart grid implementation successful. More specifically, the paper highlights the cyber-security issues in key areas of architecture, communication protocol, interfaces, home area networks, human factors, physical security, and different ICT components. The study finally gives the state of the art solutions to deal with the mentioned cyber-security issues for improving smart grid security.

## References

1. Zhou J, He L, Li C, Cao Y, Liu X, Geng Y (2013) What's the difference between traditional power grid and smart grid?—From dispatching perspective. In: IEEE PES Asia-Pacific power and energy engineering conference (APPEEC)
2. Bari A, Jiang J, Saad W, Arunita J (2014) Challenges in the smart grid applications: an overview. Int J Distrib Sens Netw 10(2)
3. Chebbo M (2007) EU smart grids framework "Electricity networks of the future 2020 and beyond". In: IEEE power engineering society general meeting, Tampa, pp 1–8
4. Tuballa ML, Abundo ML (2016) A review of the development of smart grid technologies. Renew Sustain Energy Rev 59:710–725
5. Mrabet ZE, Kaabouch N, Ghazi NE, Ghazi HE (2018) Cyber-security in smart grid: survey and challenges. Comput Electr Eng 67:469–482
6. Wang W, Lu Z (2013) Cyber security in the smart grid: survey and challenges. Comput Netw 57(5):1344–1371
7. Bigerna S, Bollino CA, Micheli S (2016) Socio-economic acceptability for smart grid development—a comprehensive review. J Clean Prod 131:399–409
8. Kappagantu R, Daniel SA (2018) Challenges and issues of smart grid implementation: a case of Indian scenario. J Electr Syst Inform Technol 5(3):453–467
9. Baumeister T (2010) Literature review on smart grid cyber security. Collaborative Software Development Laboratory at the University of Hawaii

10. Wang W, Xu Y, Khanna M (2011) A survey on the communication architectures in smart grid. Comput Netw 55:3604–3629
11. Yang Y, Littler T, Sezer S, McLaughlin K, Wang HF (2011) Impact of cyber-security issues on smart grid. In: 2nd IEEE PES international conference and exhibition on innovative smart grid technologies, Manchester
12. Pearson ILG (2011) Smart grid cyber security for Europe. Energ Pol 39(9):5211–5218
13. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on cyber security for smart grid communications. IEEE Commun Surv Tutorials 14(4):998–1010
14. Aillerie Y, Kayal S, Mennella JP, Samani R, Sauty S, Schmitt L (2013) White paper: smart grid cyber security. Intel, ALSTOM and McAfee
15. Berthier R, Sanders WH, Khurana H (2010) Intrusion detection for advanced metering infrastructures: requirements and architectural directions. In: First IEEE international conference on smart grid communications
16. Sou KC, Sandberg H, Johansson KH (2013) On the exact solution to a smart grid cyber-security analysis problem. IEEE Trans Smart Grid 4(2):856–865
17. Abdulatif A, Kumarage H, Khalil I, Atiquzzaman M, Yi X (2017) Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure. IET Wirel Sens Syst 7:182–190
18. Yu X, Cecati C, Dillon T, Simões MG (2011) The new frontier of smart grids. IEEE Ind Electron Mag 5(3):49–63
19. Setiawan AB, Syamsudin A, Sasongko A (2015) Implementation of secure smart grid as critical information infrastructure in Indonesia: a case study in smart grid electricity. In: Fourth international conference on cyber security, cyber warfare, and digital forensic (CyberSec), pp 34–39