Evaluation of Cyber Security in Smart Grid Networks

Md Sabbir Hosen[1], Sucheta Bhowmick[2]

[1]*Department of Information & Communication Engineering, University of Science & Technology Beijing, China*
[2]*Department of Control Science & Engineering, Beihang University, Beijing, China*

---***---

Abstract - *Cyber-security is the concept of protecting the confidentiality, integrity, and availability of information resources against attacks exploiting weaknesses in information assets. Because of this, it is essential to ensure the confidentiality, integrity, and availability (CIA) of information, which are the three most important aspects of cybersecurity. Cyber security risks & cyber-attacks are key concern in today's significant infrastructures. Smart Grid Communication Networks are notable for their sharing data, improving capacity in generating, transmitting, and distributing electric power, which is one of the key characteristics of critical infrastructures. The increasing deployment of smart grid networks necessitates the identification and classification of threats, as well as the implementation of countermeasures. Cyber-attacks on smart grid communication networks necessitate the highest level of information safety. In this regard, this article introduces different types of attackers, attack classifications in smart grid networks, and large-scale cyber-attacks on electric power systems. Additionally, the article discusses the prime goals & requirements for cybersecurity in smart grid networks. Also, attacks on smart grid communication networks are classified utilizing CIA paradigms.*

***Key Words*: Cyber Security, IoT Security, Smart Grid Networks Security.**

1.INTRODUCTION

The Internet of Things idea is revealed when devices are managed via the internet infrastructure (IoT). The Internet of Things (IoT) can be described as a communication network consisting of physical objects that interact with one another utilizing a variety of communication protocols [10]. There is a variety of Internet of Things applications, including smart cities, smart homes & smart transportation. The idea of the smart grid communication network is revealed when conventional electricity networks are connected with the Internet of Things (IoT) technology [13]. Conventional Electric power networks have been brought up to date by Smart Grid Networks. Smart grid networks require real-time monitoring of characteristics such as frequency, power, voltage, and current in order to operate effectively. This implies that the system's linked components may autonomously optimize their operations, monitor themselves, and defend themselves against cyber-attacks [1]. There are two types of transmission lines in a smart grid communication network: power transmission line and data transmission line [7].

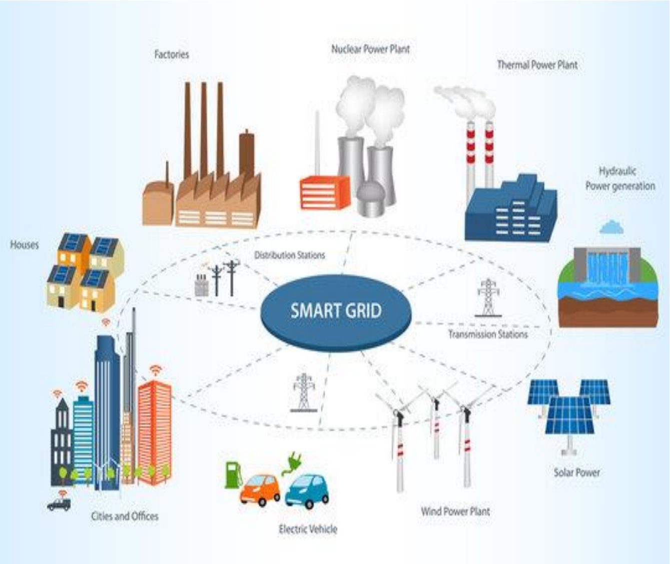

Fig -1: Smart Grid Networks Architecture

The communication infrastructure is responsible for coordinating and transferring data between network components in a bidirectional method. It is becoming more challenging to manage the communication infrastructure due to integrating various technologies, such as energy storage technologies, renewable energy sources, electric cars, and remote reading systems, into smart grid communication networks [11]. As a result, maintaining data security in smart grid networks, which are cyber-physical systems, becomes a challenge. Because of this, three fundamental security principles - confidentiality, integrity, and availability - must be observed in order to guarantee the security of all cyber-physical systems [1]. The importance of providing integrity, availability, and confidentiality, which are the main components of cyber-security in smart grid communication networks, has been explored in this article.

2. INFORMATION SECURITY OF SMART GRID NETWORKS

Each type of data generated by smart grid networks plays a vital role in enhancing the human life, both in terms of their generation and energy consumption. To prevent cyber-attacks that may occur during the collecting and distribution of data, it is necessary to implement information security in operation [6]. Data security precautions are commonly defined as the provision of data integrity, confidentiality, and availability. The expected benefits from smart grid communication networks depend on the ability to communicate data efficiently and securely between the parties involved in the network efficiently and securely [8]. The provision of security for communication channels and AMI(Advanced Metering Infrastructure) can be considered to be the primary means of ensuring the security of smart grid networks [2]. In smart grid communication networks, there are seven distinct domains [3]. These seven domains, in which they all communicate with one another. Each of these seven domains' interfaces has a unique set of security needs regarding the data's availability, integrity, and confidentiality, which are all different from one another.

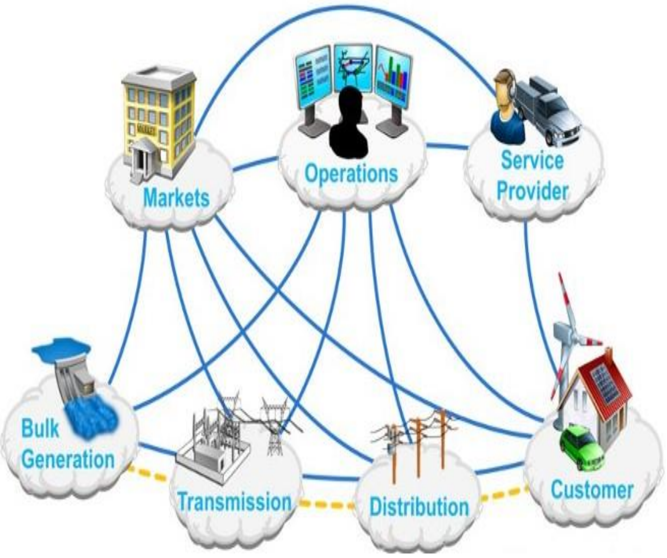

Fig -2: Smart Grid Networks Domains

Moreover, privacy, access to high-quality data, preventing unwanted access, assuring system continuity, and providing high-quality service are criteria for cyber-security in the smart grid networks domains.

2.1 Attacker Types in Smart Grid Networks

It is possible for attackers or users, either consciously or unconsciously, to take advantage of vulnerabilities in smart grid networks to cause damage at various levels of the system for various purposes. Customers who want to lower their electricity bills can target specific system components by connecting to the nearest Advanced Metering Infrastructure system [8]. This is all it takes for these attackers to reduce their electricity bills. Some end-users may also wish to provide financial benefits to the system by changing their generation and consumption information or by gaining access to the billing system, among other options. Attackers are classified based on the targets and motivations that they pursue [1]. Cyber-attacks on smart grid networks can be motivated by various factors, including cyber warfare, terrorism, industrial espionage, activism, economic reasons, disgruntled employees, and even jokes [12]. Those who carry out the attacks can be anyone – amateurs or professionals – including terrorists, employees, competitors, and even customers themselves. Non-malicious attackers are those who are curious about the system and whose primary goal is not to cause harm to it. They approach the problem of system security and operation as if it were a puzzle to be solved. These assailants act with a sense of intellectual curiosity and challenge. Script kiddies and hobbyists are generally considered to be harmless attackers in smart grid communication networks [5]. Some attackers who seek to gain a personal advantage may also pose as malicious customers in some cases. These end-users can take advantage of their smart meters or data transmission lines in a way that is advantageous to them [12]. When terrorists launch attacks on electric power grid systems, they hope to disrupt the operation of critical infrastructure, increase the effectiveness of their terrorist actions, and cause widespread disruption of public order. Some employees, particularly those who are engaged with customers or their employers, may choose to attack the system deliberately [14]. In addition, a disgruntled employee who has been granted access to system components may alter the settings of software algorithms or the configurations of devices to suit their own interests and benefit. The term "internal attackers" is frequently used to describe this unhappy personnel. Competitors can also wage war on one another for the sake of financial benefit. For example, corporate data or private consumer data may be taken from a database because of the competition between service providers [9]. Competitor attackers are the term used to describe this type of attacker. State hackers, organized criminal attackers, and hacktivists are examples of diverse types of attackers with various motivations. Smart grid networks are at the nexus of intelligence, energy, politics, and social concerns, which helps to understand the wide range of attackers and their goals on these networks [10]. As a result, there may be more attackers with a variety of attack motivations.

2.2 Attack Types in Smart Grid Networks

Physical threats, environmental threats, and cyber threats are the three types of threats that can affect an electric power system [15]. On the other hand, physical threats include unauthorized threats to physical accessibility, whereas environmental threats include threats such as natural disasters, extreme heat, and cold, among other things. As cyber-physical systems, smart grid networks are examined in this article, which focuses on the threats to the cyber component of smart grid communication networks. Attacks on smart grid networks are primarily motivated by three factors: manipulation, sabotage, and espionage [1]. They can be carried out voluntarily or unintentionally in this manner. Deliberate attacks are those that are carried out with the intent of causing damage to the availability, confidentiality, and integrity principles of a system [13]. Hackers, organized crime, cybercrime, terrorists, anti-government organizations, and vandals are all examples of deliberate attackers. Furthermore, end-users who have smart meters may attempt to attack the energy infrastructure for various reasons, including energy theft, fraud, sabotage, and vandalism, to name a few [7]. A deliberate attack is when the perpetrator is not aware that he or she is committing a cyber security breach. These attacks are typically committed by end-users who are uninformed about cyber security issues. These users are frequently duped by malicious attackers who are fully aware of their actions and intentions. In some cases, these attacks can cause significant damage to the system.

It is known that there are two types of security attacks that can be used to compromise the security of Smart Grid Networks:

1) Passive Attacks: Obtaining the transmitted data is the attacker's goal to know the system's configuration, architecture, and expected behavior. Since there is no change in the data, it is difficult to identify such attacks. As a result, rather than focusing on passive attack detection, the emphasis should be placed on passive attack prevention instead. Passive attacks such as eavesdropping, and traffic analysis are examples of this type. In the case of passive attacks, the confidentiality principle is violated [1].

2) Active Attacks: An active attack attempts to interfere with the system's operation by changing the transmitted data or inserting altered data into the system. In the case of an active attack, one or more of the following standards are violated: availability, integrity, or partially confidentially. Whether knowingly or unintentionally, other parties carry out passive and active attacks on the victim [1].

3. SMART GRID NETWORKS SECURITY PRINCIPLES

A smart grid communication system must be capable of supporting all or parts of the data sharing, power generation, distribution, transmission, and control operations. It is necessary to enable the main security objectives as well as bidirectional communication to ensure that these transactions communicate safely [1]. It is also necessary to provide a layered communication architecture with a secure communication channel. Smart grid networks are made up of a large number of devices that are all interconnected.

There are two types of data that are transmitted between these devices.

User Data: This term refers to data that concerns one's privacy, such as user information, consumption data, log data, and report data. The collection of such information by attackers almost always entails a violation of privacy.

Operations & Maintenance Data: It consists of a set of guidance that contain commands and control. In order to protect smart grid communication networks from attacks that could result in data transmission & power outages, operations and maintenance data must be protected at the highest level of security possible [8]. The current loads of transformer feeders, transformer tap changers, capacitors, fault sites, the status of relays, the real-time current and voltage values, the status of circuit breakers, and other operational data are displayed in the operations & maintenance data. The capture of such data by attackers has the potential to do significant damage to the operation of the entire system [12].

The confidentiality, integrity, and availability of data are the three primary security objectives [1]. Confidentiality is the protection of personal data from unauthorized access. The integrity of data ensures that it is accurate. The availability of the services ensures that the services will be accessible [2]. However, in traditional communication networks, the significance order of security requirements is CIA (Confidentiality, Integrity, and Availability), whereas, in smart grid networks, the importance order is AIC (Availability, Integrity, and Confidentiality) [1].

Three essential security principles must be strictly adhered to in smart grid communication networks. As a result, availability, integrity, and confidentiality in smart grid networks must all be ensured [13].

1) Availability: It is responsible for ensuring that authorized parties have access to the information when it is needed. It assures that unauthorized persons or devices will not be able to access the system. In Smart Grid Communication Networks, availability refers to the state of all cyber systems, including Supervisory Control and Data Acquisition (SCADA), Distributed Control Centers (DCC), and Distribution Management Systems (DMS), as well as the communication networks that connect these systems to external networks [7]. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks are designed to reduce the availability of a system [4]. As a result, they seek to cause data transit to be delayed, prevented, or disrupted in smart grid networks. Blackouts, brownouts, and denial of data exchange are all caused as a result of this situation [5]. The failure of control messages or the inaccessibility of the data stream harms the power distribution and the network. As a result, availability is widely regarded as the most crucial cyber-security need in a Smart Grid Network.

2) Integrity: Sensors, control commands, software, and electronic devices containing essential data are protected from tampering to prevent data exchange and decision-making disruption [10]. The integrity of source validation and software updates should be ensured by smart meters. During the transfer of smart meter data to the distribution company, it may be vulnerable to an attack that compromises the integrity of the data [2]. When transmission data is used for billing purposes, the integrity of the data must be maintained. The unauthorized alteration of this data, on the other hand, may result in financial loss for either the company or the end-user. Data flow, control messages, and sensor values that have been maliciously altered or repeated indicate that the system is attacked [12]. Integrity has been compromised in this manner. The unauthorized alteration and destruction of data constitute a loss of integrity of the data. The system responsible for power management may make incorrect decisions as a result of these circumstances. Data integrity is dependent on the non-repudiation and authenticity of the data [1]. An integrity attack is a cyberattack that aims to change customer information such as their account information, billing information, or network operation data such as the operating status of devices and voltage readings [15]. In other words, such attacks attempt to deliberately alter the original data in the smart grid communication system to disrupt critical data exchange in the smart grid networks.

3) Confidentiality: It is ensured that only the appropriate receivers have access to the data that has been stored and transmitted [1]. To protect personal privacy and security, confidentiality also prevents unauthorized users from accessing data. Consumer-specific data is transmitted through smart grid networks with varying levels of sensitivity and privacy protection [9]. It is only appropriate for the end-user and the energy provider to have access to an end user's consumption data. The system may be compromised if attackers capture control messages or data streams from it. Confidentiality refers to the protection of confidential information from being disclosed to unauthorized users [14]. From the perspective of smart grid networks, this refers to the privacy of customer data, electric market data, and critical enterprise data. When private information is revealed, it results in a breach of confidentiality. Due to the increasing accessibility of customer data on the Internet, the importance of confidentiality is becoming increasingly important [2].

3.1 Smart Grid Networks Security Requirements

Aside from the availability, integrity, and confidentiality requirements, some additional security requirements must be met in conjunction with the essential security components of smart grid networks.

Data protection: User data must not be used for different reasons without the user's permission, and it must not be obtained by different people or be used for purposes other than those stated in the privacy statement. For example, data on energy use that is utilized for billing purposes cannot be used for any other reason.

Authorization: The authentication of an object or person assures that the object or person has specified permissions to conduct specified activities on specific resources. For example, an officer who is responsible for manually configuring a smart meter must be granted predefined authorization and access control privileges before beginning his work.

Verification: Verification that a specific action made by a system or user cannot be undone later on is undertaken. Ultimately, the purpose of verification is to establish that a specific communication is associated with a specific entity.

Recognition: It is the way to recognize a system user or an application that is uniquely running on the system.

Identity Management: Authentication is the capacity to demonstrate that a user or application is, in fact, who or what the user or program purports to be. It establishes the identification of the user or client machine attempting to log in to the system.

Access Management: System and network resources are managed through the use of a system called access control. User authentication allows them to access specific resources based on the policies of their respective organizations. It is frequently used in conjunction with authentication.

Security Evaluation: An information system's security is evaluated comprehensively by analyzing how well it conforms to a set of established standards. The physical configuration environment, procedures, user practices, information management, and software are all evaluated as part of a comprehensive audit. Compliance with security policies is ensured through auditing, which checks both users and administrators. Accountability can be established through the use of security evaluation.

Specific security criteria are required for the protection of cyberinfrastructure in order to reduce liability and promote competence in the electric marketplace. As a result, any weaknesses in security essential aspects and requirements may result in significant cyber or even physical security problems of smart grid networks.

3.2 Smart Grid Networks Cyber Attacks Classification

Malicious software includes viruses, spyware, worms, trojans, logic bombs, back-doors, and trapdoors, to name a few examples. Developers can intentionally embed logic bombs, back doors, and trapdoors into software, which can then be used to launch attacks later. DoS or distributed denial of service (DDoS) attacks attempt to delay, obstruct, or damage information transmission and exchange between nodes in a Smart Grid Network [2]. Man-in-the-middle attacks, message replays, spoofing, and software exploitation are all examples of spoofing attacks[1]. Attacks against the man in the middle may be carried out in multiple layers. An attacker only needs to establish a connection to the communication channel to launch a jamming attack. A zero-day attack is a cyberattack that exploits a previously unknown security vulnerability that is only discovered after the attack has been completed. Eavesdropping is a passive attack in which the attacker overhears messages sent between two nodes over a communication line [7]. Wormhole, flooding, denial of service, distributed denial of service, jamming, buffer overflow, and puppet attacks all cause damage to the availability principle in the smart grid network[1]. Wormhole, data tampering, data injection, spoofing, and time synchronization attacks all cause damage to the integrity principle in the smart grid network[3]. Attacks such as man in the middle, password pilfering, spoofing, traffic analysis, and unauthorized and eavesdropping interfere with the confidentiality principle in the smart grid network [2].

4. CONCLUSIONS

Cyber-security incidents and academic papers highlight that many potential cyber-attacks are becoming increasingly likely on systems as complicated and diverse as the emerging smart grid network. Additionally, new technologies and the active participation of customers in smart grid networks may result in security threats. Therefore, it is necessary to improve the system by constructing a robust and effective smart grid cyberinfrastructure. It will be easier to develop practical solutions for current and future cyber-attacks on smart grid networks if cyber-attacks are classified according to the key elements of information security. Furthermore, because of the unique characteristics of smart grid networks, customized solutions must be developed for each network's specific requirements.

REFERENCES

[1] M. Z. Gunduz and R. Das, “A comparison of cyber-security-oriented testbeds for IoT-based smart grids,” in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–6, Mar. 2018.

[2] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, “A Survey on Smart Grid Cyber-Physical System Testbeds,” IEEE Communications Surveys Tutorials, vol. 19, no. 1, pp. 446–464, 2017.

[3] E. U. Haq, H. Xu, L. Pan, and M. I. Khattak, “Smart Grid Security: Threats and Solutions,” in 2017 13th International Conference on Semantics, Knowledge and Grids (SKG), pp. 188–193, Aug. 2017.

[4] C. Bekara, “Security Issues and Challenges for the IoT-based Smart Grid,” Procedia Computer Science, vol. 34, pp. 532–537, Jan. 2014.

[5] L. Kotut and L. A. Wahsheh, “Survey of Cyber Security Challenges and Solutions in Smart Grids,” in 2016 Cybersecurity Symposium (CYBERSEC), pp. 32–37, Apr. 2016.

[6] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, “Smart grids security challenges: Classification by sources of threats,” Journal of Electrical Systems and Information Technology, Feb. 2018.

[7] R. K. Pandey and M. Misra, “Cyber Security Threats-Smart Grid Infrastructure,” in 2016 National Power Systems Conference (NPSC), pp. 1–6, Dec. 2016.

[8] C. P. Vineetha and C. A. Babu, “Smart grid challenges, issues and solutions,” in 2014 International Conference on Intelligent Green Building and Smart Grid (IGBSG), pp. 1–4, Apr. 2014.

[9] D. B. Rawat and C. Bajracharya, “Cyber security for smart grid systems: Status, challenges and perspectives,” in SoutheastCon 2015, pp. 1–6, Apr. 2015.

[10] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, “Smart grid security issues,” in 2015 9th International Conference on Compatibility and Power Electronics (CPE), pp. 534–538, June 2015.

[11] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. A. Ali, “Smart grid cyber security: Challenges and solutions,” in 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 170–175, Oct. 2015.

[12] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 981–997, 2012.

[13] A. Procopiou and N. Komninos, “Current and future threats framework in smart grid domain,” in 2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 1852–1857, June 2015.

[14] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A Survey on Cyber Security for Smart Grid Communications,” IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 998–1010, 2012.

[15] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” Computer Networks, vol. 57, pp. 1344–1371, Apr. 2013.

BIOGRAPHIES

MD SABBIR HOSEN received the bachelor's degree in Electronics & Telecommunication Engineering from Daffodil International University, Bangladesh, in 2018. He is currently pursuing the master's degree with the School of Computer & Communication Engineering, University of Science & Technology Beijing, China. His research interests focus on Cognitive Radio Networks and Smart Grid Networks.

SUCHETA BHOWMICK received the bachelor's degree in Computer Science & Engineering from Stamford University Bangladesh. She is currently pursuing the master's degree with the School of Automation Science & Electrical Engineering, Beihang University, Beijing, China. Her research interests focus on Cyber Security, Pattern Recognition and Computer Vision.