Journal of The Gujarat Research Society
ISSN: 0374-8588
Volume 22 Issue 1, January 2020

An Overview Of Cyber Security In Smart Grid

Prof. (Dr.) Tarun Kr. Sharma, Dr. Mamta Bansal
Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- tarun.sharma@shobhituniversity.ac.in, mamta.bansal@shobhituniversity.ac.in

ABSTRACT: ***A smart grid harnesses the power of information technology to intelligently provide energy to consumers through two-way communication while also meeting environmental standards via the integration of green technologies. Despite the fact that smart grid solves many issues with conventional grids, it faces a number of security issues. Because communication has been integrated with electrical power, which has inherent flaws, the system has been exposed to many dangers. These issues have been addressed in a number of academic publications. However, the majority of them categorized attacks based on confidentiality, integrity, and availability, while excluding assaults that jeopardized other security criteria like accountability. Furthermore, existing security countermeasures are focused on preventing particular attacks or safeguarding certain components, but there is no comprehensive strategy that brings these solutions together to defend the whole system. The goal of this article is to provide a thorough review of the relevant published studies. We start by going through the security needs. Then, to identify possible weaknesses and their effect, we look at a number of major cyber-attacks in the smart grid in detail. We also suggested a cyber security plan as a method for dealing with breaches, preventing attacks, and deploying suitable remedies. Finally, we suggest some study topics for the future.***

KEYWORDS: ***Cyber-Attacks, Confidentiality, Cryptography, Smart Grid, Vulnerabilities.***

1. INTRODUCTION

Traditional electrical distribution systems transmit electrical energy produced at a central power plant by raising voltage levels and then progressively lowering voltage levels to distribute it to end customers[1]. This electrical grid, on the other hand, has many flaws, including the inability to include varied generating sources such as green energy, high costs and costly assets, time-consuming demand response, high carbon emissions, and blackouts. According to a study performed by experts at the Berkeley National Laboratory in 2004, power outages cost the American economy around $80 billion per year; other estimates put the cost at $150 billion per year[2]. It is clear that the current energy system will not be able to solve these important issues. By allowing the integration of new power resources (such as renewable energy, wind, and solar energy), providing remedial capabilities when faults occur, lowering carbon footprint, and minimizing energy losses within the system, the smart grid promises to offer flexibility and dependability[3].

In the production, distribution, and consumption of electric power, a smart grid is a system based on communication and information technologies. It utilizes a two-way information flow to build an automated and broadly dispersed system with new capabilities including real-time control, operational efficiency, grid resilience, and greater integration of renewable technologies, all of which help to reduce carbon emissions. However, there are dangers with the smart grid. Any disruptions in power production may jeopardize smart grid stability and have significant socioeconomic consequences. Furthermore, since important data is shared across smart grid devices, data theft or modification may compromise customer privacy. Smart grid has become a major target of attackers as a result of these flaws, attracting the attention of government, business, and academics. Several research articles have been published that give an overview of the current cyber security issues in smart grid infrastructure. Research of the difficulties that smart grid security faces in[4]. They divided assaults into three categories: home area network (HAN), neighborhood area network (NAN), and wide area network (WAN)

(WAN). They also discussed the effect of each assault on information security, including confidentiality, integrity, and availability (CIA)[5].

Smart grid security issues in, particularly those relating to connection, trust, consumer privacy, and software vulnerabilities[6]. The writers also included a rundown of current security solutions, including network security, data security, key management, network security protocols, and compliance checks[7]. The paper proposes a smart grid protection architecture based on a public network. There were three levels to this framework: the main station, the communication network, and the terminals. Dari et al. addressed the security needs and risks to the smart grid in. Three types of risks were identified: people and policy, platform, and network threats. Wang et al. categorized attacks based on CIA criteria in, and they detailed a variety of countermeasures, including network security, cryptography, secure protocols, and secure design. While these survey studies classify smart grid threats in a variety of ways, the majority of them are based on confidentiality, integrity, or availability[8].

Blended and sophisticated assaults like Stuxnet, Duqu, and Flame may, on the other hand, compromise all of the security criteria at the same time. As a result, such assaults are often left out of these categorization schemes. Furthermore, countermeasures and security solutions were provided separately for each component of the smart grid, and there is no unified strategy or procedure for combining these security mechanisms to guarantee system security. This paper summarizes the present state of smart grid cyber security as well as future expectations. The rest of this paper is laid out as follows. First, we'll go through the smart grid's cyber security goals. Following that, we propose a new cyber-attack categorization system based on a technique employed by hackers or penetration testers. This approach enables a better understanding of how a hacker compromises the smart grid's security. After that, we summarize and suggest a few countermeasures. In the last part, several difficulties and potential directions are addressed[9].

1.1 Overview Of Smart Grid :

- *The advantages of a smart grid* : The smart grid's primary advantages are anticipated to be increased system resilience and improved environmental performance. Resilience refers to an entity's capacity to withstand and recover swiftly from unforeseen occurrences. Grid resilience has become an unavoidable element in today's world, particularly when power outages threaten the economy. By allowing more distributed power supply, easing the integration of new resources into the grid, and providing remedial capabilities when problems arise, the smart grid promises to bring flexibility and dependability. Furthermore, smart grid technologies are anticipated to allow electric cars to replace conventional vehicles, lowering customer energy consumption and decreasing grid energy losses[10].
- *The conceptual model of a smart grid*: A smart grid, according to the National Institute of Standards and Technology (NIST) is made up of seven logical domains that comprise both actors and applications: bulk generation, transmission, distribution, customer, markets, service provider, and operations. Programs, devices, and systems are actors, while applications are tasks carried out by one or more actors in each domain. The smart grid conceptual model and the interaction of players from many domains through a secure channel. The end user is the primary actor in the customer domain. Customers are divided into three categories: residential, commercial/building, and industrial. These actors have the ability to produce, store, and manage energy in addition to consuming it. This domain interacts with the distribution, operation, service provider, and market domains and is electrically linked to the distribution domain.

Actors in the market sector are power market operators and participants. This domain keeps the supply and demand of electricity in check. The market domain interacts with energy supply domains such as the bulk generating domain and distributed energy resources (DER) in order to match output with demand. Organizations that offer services to both electrical consumers and utilities fall under the service provider domain. Billing, client accounts, and energy use are all managed by these companies. The service provider connects with the operation domain for situational awareness and system control, as well as with the customer and market domains to create smart services such allowing customers to engage with the market and generate energy at home. The players in the operations domain are the people in charge of moving electricity.

- *The systems of the smart grid* : Advanced metering infrastructure (AMI) , automated substation , demand response, supervisory control and data acquisition (SCADA), electrical vehicle (EV) , and home energy management (HEM) are some of the dispersed and heterogeneous applications that make up the smart grid. We'll talk about three important and susceptible smart grid applications in this section: AMI, SCADA, and automation substation go through the various uses in great depth. The advanced metering infrastructure (AMI) collects, measures, and analyzes electricity, water, and gas consumption. It provides for two-way communication between the utility and the user. There are three parts to it: the smart meter, the AMI headend, and the communication network . Smart meters are digital meters with microprocessors and local memory that are used to monitor and collect power consumption from home appliances as well as send data in real time to the utility's AMI headend. The meter data management system (MDMS) makes up an AMI headend, which is an AMI server. Several communication protocols, such as Z-wave and Zigbee, specify communication between smart meters, household appliances, and the AMI headend.
- *Network protocols for smart grids* : Different communication protocols are required for distributed and heterogeneous applications in the smart grid. The smart grid network design and protocol utilized inside each network. Home appliances utilize the ZigBee and Z-wave protocols in the home area network (HAN). The IEEE 802.11, IEEE 802.15.4, or IEEE 802.16 protocols are often used to link devices in a neighborhood area network (NAN). Several industrial protocols, including distributed networking protocol 3.0 (DNP3) and modicon communication bus (ModBus), are used in wide area network (WAN) and supervisory control and data acquisition (SCADA) applications . Protocol IEC 61850 is used in substation automation. Modbus and DNP3 are two commonly used yet susceptible smart grid protocols that will be discussed in this section. go through Bluetooth, Z-Wave, Zigbee, 6LoWPAN, WiMAX, the IEC 61850 standard, and power line communication in detail. Modicon communication bus (ModBus) is a seven-layer OSI protocol that was created in 1979 to allow process controllers to interact with computers in real time. Modbus is divided into three types: Modbus ASCII, Modbus RTU, and Modbus/TCP. Messages are encoded in hexadecimal in the first. It is excellent for radio connections and telephone conversations, despite its slowness. The messages in the second one are encoded in binary and sent through RS232. The masters and slaves communicate via IP addresses in the third one . ModBus is a master-slave protocol used in SCADA systems to exchange commands between a master, also known as a remote terminal unit (RTU) or master terminal unit (MTU), and multiple slave devices, such as sensors, drivers, and PLCs . On the one hand, Modbus is extensively used in industrial architecture

because to its relative simplicity of use in transmitting raw data without the need for authentication, encryption, or any additional complexity.

1.2 need of smart grid security :

The National Institute of Standards and Technology (NIST) has established three criteria for maintaining and protecting information security in the smart grid, namely confidentiality, integrity, and availability. Accountability is another essential security requirement. Each criterion is described in detail below.

- *Confidentiality*: In general, confidentiality protects approved information access and disclosure limitations. In other words, the confidentiality criteria necessitate preventing unauthorized organizations, people, or processes from accessing or disclosing personal or private information. Confidentiality is lost whenever information is disclosed without authorization. For example, information transmitted between a customer and different organizations, such as meter control, metering use, and billing information, must be private and safeguarded; otherwise, the customer's information may be manipulated, edited, or used for other harmful reasons.
- *Accessibility*: The term "availability" refers to the capacity to get and utilize information in a timely and accurate manner. Because loss of availability implies interruption of access to information in a smart grid, it is regarded the most critical security criteria in smart grid. For example, a lack of availability may disrupt the control system's functioning by preventing information from flowing over the network and therefore denying the network's availability to the system's operators.
- *Integrity*: In the smart grid, integrity refers to safeguarding data against unauthorized alteration or deletion. A loss of integrity occurs when data is tampered with, modified, or destroyed without being noticed. Power injection, for example, is a malicious assault carried out by an adversary who cleverly changes measurements and transmits them to the state estimator from the power injection meters and power flow. To preserve the integrity, both nonrepudiation and information veracity are needed. Nonrepudiation refers to the inability of people, entities, or organizations to undertake a certain activity and then deny it afterwards; authenticity refers to the fact that data comes from a genuine source.
- *Accountability*: Accountability implies that the system is traceable and that every action taken by a person, gadget, or even a government agency is recorded so that no one can dispute what they did. This observable data may be used as evidence in a court of law to identify the perpetrator. Customers' monthly energy bills are an example of an issue with accountability. Smart meters, in general, may calculate the cost of energy in real-time or on a daily basis. However, if these meters are under assault, the data they provide is no longer accurate since they have been compromised. Smart grid network design has changed. As a consequence, the consumer will get two energy bills: one from the smart meter and one from the utility.

1.3 Smart Grid Attacks:

Reconnaissance, scanning, exploitation, and maintaining access are the four stages used by malevolent hackers to attack and gain control over a system. The attacker acquires and collects information about its target during the first stage, reconnaissance. The attacker attempts to discover the system's weaknesses in the second phase, scanning. These activities are designed to detect the open ports and to learn about the services that are operating on each one, as well

as their flaws. He/she attempts to compromise and gain complete control of the target during the exploitation stage. After gaining administrator access to the target, the attacker must complete the last stage, which is to keep the access. This is accomplished by installing a covert and undetected software, allowing him/her to simply return to the target system later. Attackers in the smart grid use the same methods to breach the security criterion. They utilize various methods to compromise a specific system in the grid at each stage. As a result, these stages may be used to classify assaults. As describe below.

- *Surveillance*: The assaults in the first phase, reconnaissance, are social. Transportation engineering and analysis Social engineering is the process of manipulating people's (SE), rather of using technology, it focuses on social skills and human connection. technical abilities. An assailant use communication and persuasion to gain a genuine user's confidence and get passwords and other sensitive information are examples of credentials and confidential information. To log in to a specific system, you'll need a PIN number. As an example, The terms "phishing" and "password pilfering" are well-known. SE methods are utilized. The traffic analysis attack is a kind of cyber-attack that is used to Listen to the traffic and analyze it to figure out what's going on. The devices and hosts connected to the network, as well as their Internet Protocol (IP) addresses Traffic analysis and social engineering Specifically, the information's confidentiality is jeopardized.
- *Examining*: The scanning attack is the next step in the process of locating all of the objects. On the network, keep the devices and hosts alive. There are four of them. IPs, ports, services, and vulnerabilities are all types of scans. In most cases, an attacker begins with an IPs scan to identify all of the computers on the network. The IP addresses of the hosts connected to the network. Then he or she digs a little deeper by scanning the ports for anything suspicious. Find out which port is open This scan is carried out on each device. On the network, a host has been discovered. The assailant then proceeds to the service scan to determine which service or system is being used running behind each port that has been opened If, for example, port 102 is used, If a hacker notices a system is open, he or she may deduce that this system is a control system for a substation or messaging.
- *Profiteering*: Malicious actions are included in the third stage, exploitation. That make an effort to take use of the smart grid component's weaknesses and regain control of the situation. These are the actions involved. Viruses, worms, Trojan horses, and denial-of-service attacks are just a few examples. Attacks such as denial-of-service (DOS), man-in-the-middle (MITM), and replay assaults, channel jamming, and the human machine being popped breaches of the human-machine interface (HMI), integrity violations, and privacy violationsa A virus is a computer software that infects a computer or a device. smart grid system. A worm is a self-replicating organism. Program. It makes advantage of the network to disseminate, duplicate, and replicate itself. Other devices and systems may be infected . A Trojan horse is a kind of horse that is used to deceive people.a software that seems to do something useful on the target system. In the background, however, it executes dangerous code. This kind of malware is used by an attacker to spread a virus or other malicious software. On the target system, there is a worm. In June of that year, Roel Schouwenberg, a Kaspersky Lab senior researcher, discovered The first worm to target supervisory control and data was Stuxnet.
- *Keeping access open*: The attacker uses a password to maintain access in the final step.A special type of attack that allows the attacker to gain permanent access to the

target Backdoors, viruses, and Trojan horses, in particular. a secret passageway is an undetectable program that is installed invisibly on the target in order to Return easily and quickly later . If the intruder is successful, embedding a backdoor into the control center's servers . He or she can use the SCADA to launch a number of attacks against it. the system that has the potential to have a significant effect on the electricity grid system. The elements of security in an IT network are categorized depending on confidentiality, importance, importance, importance, importance, importance, importance, importance, importance, importance, importance, importance, importance Integrity, accountability, and accessibility are all values that we hold dear. In the smart grid, they are classified as follows: availability, integrity, accountability, and responsiveness. as well as discretion.

2. DISCUSSION

Different devices coexist and communicate through various network protocols in heterogeneous systems like the smart grid. This heterogeneity is both a challenge and a potential threat to the security of the smart grid. The exchange of data between devices necessitates data aggregation and protocol translation. However, because a feature in one protocol could not be properly translated into another, this aggregation can lead to unintentional breaches and vulnerabilities. Furthermore, the majority of industrial network protocols used in smart grids, such as DNP3, ICCP, Modbus, and Profibus, were designed for connectivity rather than security. As a result, these protocols are not only unable to provide a secure communication channel, but they can also be exploited as an attack surface. Though some industrial protocols, such as secure DNP3, have secure versions. The issue with this new version is that it is incompatible with existing installations. In addition to network protocols, smart grid operating systems and physical equipment may be vulnerable, making the system vulnerable to a variety of attacks. Operating systems lack security features because they are designed for control in automation control components. Furthermore, the majority of physical devices are obsolete, and others have insufficient memory and computational capacity to support advanced security mechanisms. Because smart meters are designed for low power consumption, they have limited memory and computational resources and thus cannot support some important security mechanisms such as proper random number generators and cryptographic accelerators. Despite the fact that these components have a lower impact on smart grid operation, if they are compromised, they represent a potential vector for the entire system to be compromised.

3. CONCLUSION

A smart grid is a system composed of dispersed and heterogeneous components that intelligently provide energy while allowing renewable technologies to be readily integrated. However, there are a lot of security flaws in this important system. In this article, we give a thorough review of smart grid cyber-security and analyze the major cyber-attacks that threaten its infrastructure, network protocols, and applications in detail. In addition, we suggest an approach that combines a number of tools and procedures to address possible component weaknesses, identify malicious activity, improve network communication security, and safeguard consumer privacy.

REFERENCES

[1] M. L. Tuballa and M. L. Abundo, “A review of the development of Smart Grid technologies,” *Renewable and Sustainable Energy Reviews*. 2016, doi: 10.1016/j.rser.2016.01.011.

[2] D. Kolokotsa, "The role of smart grids in the building sector," *Energy and Buildings*. 2016, doi: 10.1016/j.enbuild.2015.12.033.

[3] M. S. Hossain, N. A. Madlool, N. A. Rahim, J. Selvaraj, A. K. Pandey, and A. F. Khan, "Role of smart grid in renewable energy: An overview," *Renewable and Sustainable Energy Reviews*. 2016, doi: 10.1016/j.rser.2015.09.098.

[4] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid - The new and improved power grid: A survey," *IEEE Communications Surveys and Tutorials*. 2012, doi: 10.1109/SURV.2011.101911.00087.

[5] N. Jenkins, C. Long, and J. Wu, "An Overview of the Smart Grid in Great Britain," *Engineering*. 2015, doi: 10.15302/J-ENG-2015112.

[6] P. Siano, "Demand response and smart grids - A survey," *Renewable and Sustainable Energy Reviews*. 2014, doi: 10.1016/j.rser.2013.10.022.

[7] X. Yu and Y. Xue, "Smart Grids: A Cyber-Physical Systems Perspective," *Proceedings of the IEEE*. 2016, doi: 10.1109/JPROC.2015.2503119.

[8] S. Supriya, M. Magheshwari, S. Sree Udhyalakshmi, R. Subhashini, and Musthafa, "Smart grid technologies: Communication technologies and standards," *Int. J. Appl. Eng. Res.*, 2015.

[9] A. Shomali and J. Pinkse, "The consequences of smart grids for the business model of electricity firms," *Journal of Cleaner Production*. 2016, doi: 10.1016/j.jclepro.2015.07.078.

[10] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," *Journal of Network and Computer Applications*. 2016, doi: 10.1016/j.jnca.2016.08.012.