International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 2 No. 1 April 2022 e-ISSN: 2808-554X

Cyber Security in Smart Grid Technology: A Systematic Review

Fifit Alfiah[1], Novi Rifkhah Prastiwi[2]
University of Raharja[1,2]
Jenderal Sudirman No.40, Cikokol, Kota Tangerang[1,2]
Indonesia[1,2]
e-mail: fifitalfiah@raharja.info[1], novi.rifkhah@raharja.info[2]

Author Notification
April 2022
Final Revised
April 2022
Published
April 2022

To cite this document:
Alfiah, F., & Prastiwi, N.R. (2022). Cyber Security in Smart Grid Technology: A Systematic Review. *International Journal of Cyber and IT Service Management (IJCITSM), 2(1),* 48-54. Retrieved from https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/79

DOI:
https://doi.org/10.34306/ijcitsm.v2i1.79

Abstract

A Smart Grid (SG) is an electrical infrastructure that functions similarly to a traditional power grid but includes scalable and ubiquitous two-way communications, timely control capabilities, large-scale integration of dispersed resources, and resource efficiency. Pervasive intelligent monitoring technologies, autonomous equipment defect detecting, and self-healing are all included in the SG. It is an intelligent infrastructure because of features such as 'Wireless Automatic Meter Reading' (WAMR), power system stability monitoring, distributed energy resource optimization, and Demand Response system applications. Given some of these distinguishing characteristics, SGs are without a doubt the world's future power infrastructure. A smart grid may link millions of people and devices in a network, necessitating its robustness, reliability, and security. Because of the long-range communication over open networks, one of the primary issues of today's innovative grid systems is security. Cybercriminals, hackers, and terrorists are attempting to assault this national infrastructure to obtain control over automated energy monitoring and remote control for personal benefit. This research article provides a complete overview of Smart Grids, including their design, methodology, and communication protocols, but the attention is mainly on the cyber-attacks that have been carried out and the remedies that have been advised for smart grids. Finally, we cover the numerous cyber security difficulties, the topics that remain unsolved in the literature and the present solution area, and prospective research gaps.

Keywords: *Demand Response System, Cyber-attacks, Smart Grid, Two-Way Communication*

1. Introduction

A Smart Grid is a development of the electric power grid based on a layered IT-driven design. SG can improve efficiency, resilience, reliability, and interoperability by integrating communication and physical systems [1]. In the interoperability of the electric grid, smart meters, sensors, and other communicating components of SG offer efficient distributed computing power. Demand response systems, distributed energy sources, remote-controlled components with fault checks, the capacity to self-heal during faults or bugs, and security against physical and cyber-attacks are all benefits of two-way communication between

consumers and power service systems in smart grids. The intelligent grid automatically provides a stable power source to handle demand and response cycles to avoid overload tripping and power outages. Cyber security in intelligent grids aims to protect communication and operational data in line with the CIA concept of Confidentiality, Integrity, and Availability[2]. The secure platform allows for precise monitoring of energy generation, consumption, and automation and real-time energy monitoring, with dependability, efficiency, and lower distribution costs. [3] The paper covers the intelligent grid's dependability, security, and stability and methods to address issues in a power system failure or contingency crisis. They conclude that cybercriminals and attackers have a high level of system understanding and are technologically proficient in disrupting service integrity, confidentiality, and availability. Governments and electricity customers must secure vital infrastructures from cyber terrorists and hackers, not just utility operators, engineers, or researchers.

2. Research Method

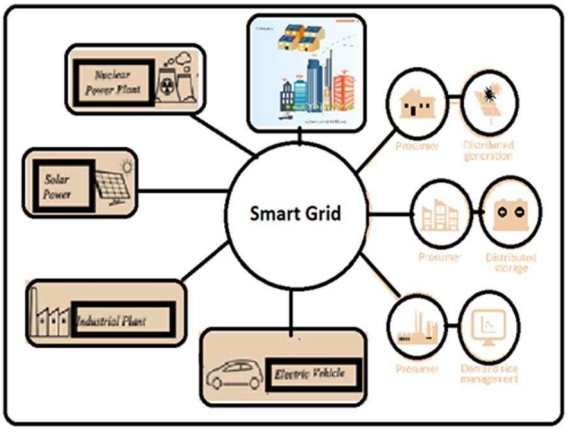
This review article aims to present a comprehensive overview of the surveys and evaluations conducted by researchers to protect communication and operational data in intelligent grids while adhering to the principles of Confidentiality, Integrity, and Availability. The main contribution is still:

- A CIA-approved assessment of a variety of existing cyber-attacks.
- Suggestions and methods for delivering adequate intelligent grid security measures are presented.
- A list of smart grid requirements and objectives.
- Providing a comprehensive overview of blockchain-based security solutions.
- Providing background information on IoT-based intelligent grids and security issues.
- Identifying a research gap that has to be filled in order to protect against unknown cyber-attacks.

3. Findings

The SG architecture is based on the National Institute of Standards and Technology's (NIST) reference model. The seven logical domains are bulk generation, HV transmission, distribution, consumers, selling and purchasing markets, operations, and electrical service providers. Distinct sorts of consumers are characterized by different networks, such as home area networks (HANs), building area networks (BANs), and industrial area networks (IANs). Advanced metering infrastructure (AMI) is implemented to track energy and communication for all inbound and outbound electrical energy flows [4]. The advanced metering infrastructure (AMI), SCADA (supervisory control and data acquisition), and communication standards and protocols are the three fundamental components of the smart grid. AMI is an intelligent link between service providers and consumers that is enabled by integrated technology. It is used for measuring consumers' energy on a real-time energy pricing system with enhanced features to help them save money on their energy bills.

SCADA is an energy management and distribution system that automates the control and monitoring of electrical systems. Significant bodies like IEEE, International Electro-technical Commission, and Distributed Network Protocol govern communication and protocol standards for power systems. To investigate intelligent grid security vulnerabilities to protect them from high-risk cyber-attacks and resulting failures. This review study assesses the numerous security concerns in the smart grid that have been explored by researchers in their research work and potential solutions.



Picture 1. Smart grid model in concept

3.1 Literature

According to the literature on smart grid cyber security, a significant number of assaults have occurred and are becoming increasingly likely on SGs [4]. Compliance is not the same as security when it comes to risk management. The goal of security is to develop a risk-managed process approach that successfully mitigates threats' vulnerabilities and reduces their potential effect to a manageable level. We must recognize that there is always some danger present; it is never zero. The remaining risk must be managed. A robust cyber security system decreases the total effect of an attack by reducing risk. The goal is to have a balanced approach; having too many security countermeasures qualifies for robust security while having too few raises weaknesses and leaves it susceptible to attackers. The correct mix of security is required. The security platform can minimize the risk and manage the danger by selecting the proper security measures in the context of the threat, vulnerability, and consequence. Countermeasures are only used when they are essential to reduce the threat. Everyone is responsible for security, just as everyone is responsible for safety. To protect the smart grid, the security program relies on the work of all components. Smart grids are also known as intelligent grids since they can interact in both directions between their units and have increased grid interoperability. The sufficient flow of data between metering equipment and substation, generation and distribution, and transmission substations with greater resilience, effective monitoring and control, and physical security are among the elements that have transformed the power system [5]. A processor provides the intelligent grid's intelligence in each system unit that runs on a stable operating system. Furthermore, components with intelligent sensors are coupled to create a vast computer platform [6]. Each unit has access to its operating system and a communication channel to a nearby unit for accessing circuit breaker functioning conditions, processor com port, and so on. The integration of large-scale dispersed infrastructure has resulted in susceptibility to physical attacks, natural disasters, and cyber-attacks, becoming a serious worry. The assaults cause significant financial loss, infrastructure failure, energy theft, privacy theft, and confusion in operating protocols, all of which impair the SGs' efficiency and dependability.

Because of the infrastructure loss it may have on sensitive national infrastructure, intelligent grid resilience against cyber-attacks is becoming critical. It must have auto-healing capabilities and superior sensing and detecting capabilities. The smart grid's cyber security is the most pressing worry, given its role in defending vital national infrastructure and hackers' expanding understanding of the cyber realm. It has been shown that some components are more vulnerable to cyber-attacks than others. Examples of more

vulnerable components include AMIs [7], exposed wireless mesh structure networks, and other attackable components. [8] discusses the threats that have increased due to the addition of new technology to smart grids. According to the literature on smart grid cyber security, a significant number of assaults have occurred and are becoming increasingly likely on SGs. Attacks against SGs are divided into attacker type and attack type. In Smart Grids, there are two sorts of attackers: The attacker's strike to inflict damage on many levels might be either conscious or unconscious. Some assaults are carried out to lower power bills, and they target their AMI or billing system. The reason for the assault and the objective of the attack may be used to categorize the attackers. Some attempt to generate conflict, while others are linked to terrorism and attempt to disrupt government operations by causing harm to critical national infrastructure. Some are unhappy personnel who aim to sabotage the utility's progress by exploiting flaws, while others do it for industrial espionage or commercial gain. Attackers can also be classified based on their knowledge of the network and infrastructure devices that are likely to be targeted by a professional attacker or an amateur attacker with no or limited knowledge of the system, and some are terrorists looking to disrupt law and order, competitors, employees, or customers [9]. Non-malicious attackers are individuals that attack only for the joy of it, without any personal or financial motivations in mind. Malicious attackers carry out assaults with a specific goal in mind.

Physical, environmental, and cyber-attacks are all types of attacks. By gaining illegal access to physical infrastructure and causing harm to the system, a physical assault poses a hazard. Cyber-attacks are attacks that manipulate calculations and readings, sabotage, and espionage the controlling and normal functioning of the system. Environment threats deal with natural threats such as natural calamities, floods, fire, extreme heat and cold, and cyber-attacks are attacks that manipulate calculations and readings, sabotage, and espionage the controlling and normal functioning of the system.

Attacks are also divided into two types based on their severity: passive and aggressive. Passive attacks breach the security concept of secrecy. Eavesdropping and network traffic analysis are two examples of such assaults. Active attacks attempt to alter existing data in the system or insert malicious material into the system to breach the security principles of availability, confidentiality, and integrity.

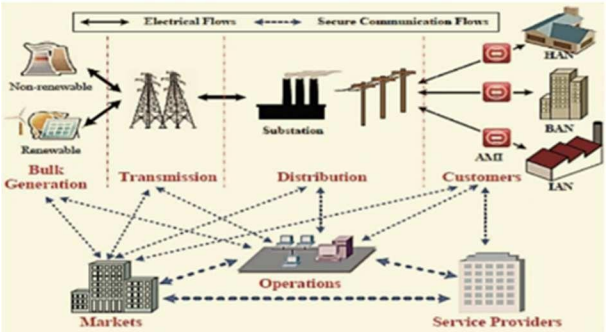
Stuxnet was one of the most significant assaults of 2011. Stuxnet was a one-of-a-kind cyber-attack. A zero-day assault goes undetected until it has completed its infectious task [10]. The Stuxnet assault was carried out against Iran's Bushehr power facilities to cause harm. It was one of the weapons employed in cyber warfare. Since this was the first malware attack on a critical infrastructure control system, it was thought to be the first of its kind. Existing cyber security systems determine that electrical energy is still vulnerable to cyber-attacks [11].

3.2 Classification Of Cyber-Attacks Usually Carried On Smart Grids

As the smart grid's communication system uses an Internet-like data network that transmits data across infrastructure overlaid on the power system using the standards of 802.15.4, 802.11, and WiMAX, it is subject to external agents' assaults. In their paper, the authors suggest a Smart Grid Distributed Intrusion Detection System [12]. Modules Analysis Security is enhanced by utilizing techniques like support vector machine (SVM) and Artificial Immune System (AIS) for identifying malicious traffic in AMs implemented at various tiers such as Home Area Networks (HANs), Wide Area Networks (WANs), and Neighborhood Area Networks (NANs)[26]. This technique has demonstrated promising

results in increasing security by detecting harmful data and determining the best communication paths.

Rather than initiating a physical attack on the power system, hackers inject erroneous data or change data. Its main goal is to change the data presented by electric power sensors rather than the actual electric power flow [13]. Because it overcomes the standard, flawed data detection approach, a severe data assault leverages system error tolerance to avoid data attack detection [14]. To counter such assaults, NIST has created a framework (see fig. 3) that is specifically tailored for cross-validating cyber and physical defensive system tactics.



Picture 2. NIST Architecture Domain

Energy Internet (EI), also known as the Internet of Energy (IoE), is the next step in the growth of the smart grid and is referred to as intelligent Grid 2.0. It is a more flexible intelligent grid integration using Internet technologies. The authors of the paper [15] investigate EI-based Internet of Things (IoT) applications in smart grids (IoT is an emerging technology with numerous advantages such as supporting heterogeneous network structures with broad application areas, the ability to communicate among various devices, and higher security features) and other innovative environments such as smart cities, smart meters, and intelligent energy management infrastructures. Furthermore, [16] identifies outstanding issues and future research possibilities in EI concepts based on IoT Infrastructures.

4. Conclusion

As hackers and cybercriminals employ new technologies to infiltrate networks and gain control of the network, or at the very least the data sent via it, threats and vulnerabilities are constantly increasing. As a result, researchers are also encouraged to improve their security approaches. The threat to intelligent grids will continue to develop as intelligent grid components (energy Internet or industrial Internet of Things) become more interconnected. From the beginning, including security in smart Grids' hardware, software, procedures, information, and media. Use the "defense in depth" approach to create mutually reinforcing controls; a single weakness will rarely be the "death chain" for hostile agents; instead, it will be a cascade of vulnerabilities and gaps in controls that will cause harm to the entire system. The most basic hack is frequently the most successful, as the human factor is both the strongest and weakest connection. This review examines and assesses the many high-potential assaults that have been carried out and are becoming more likely on Smart grids. Cyber-attacks in smart grids have risen due to the usage of new technologies with characteristics such as two-way communication between customers and the grid. It is claimed that the CIA trinity of the system has to be improved

to identify and prevent cyber-attacks on these critical national facilities. This may be accomplished by dynamically constructing a stable and robust cyber architecture in these intelligent grids. Furthermore, cyber-attacks were classed according to their behavior, key areas where and how they impacted the system, and the actions needed to give efficient and dependable responses.

References

[1] B. Chen, J. Wang, and M. Shahidehpour, "Cyber–physical perspective on smart grid design and operation," *IET Cyber-Physical Systems: Theory & Applications*, vol. 3, no. 3, pp. 129–141, 2018.

[2] D. Immaniar, N. Azizah, D. Supriyanti, N. Septiani, and M. Hardini, "PoTS: Proof of Tunnel Signature for Certificate Based on Blockchain Technology," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1 SE-Articles, pp. 101–114, May 2021, [Online]. Available: https://iiast-journal.org/ijcitsm/index.php/IJCITSM/article/view/28

[3] M. Z. Gündüz, A. Karabiber, and T. B. M. Y. Okulu, "An Overview of Smart Grid Domains and Priority Research Areas".

[4] A.-S. K. Pathan, "Attack Severity–Based Honeynet Management Framework," in *The State of the Art in Intrusion Prevention and Detection*, Auerbach Publications, 2014, pp. 103–132.

[5] M. Khan and T. Naz, "Smart Contracts Based on Blockchain for Decentralized Learning Management System," *SN Computer Science*, vol. 2, no. 4, pp. 1–9, 2021.

[6] F. Agustin, S. Syafnidawati, N. P. Lestari Santoso, and O. G. Amrikhasanah, "Blockchain-based Decentralized Distribution Management in E-Journals," *Aptisi Transactions On Management*, vol. 4, no. 2, pp. 107–113, 2020.

[7] F. Agustin, F. P. Oganda, N. Lutfiani, and E. P. Harahap, "Manajemen Pembelajaran Daring Menggunakan Education Smart Courses," *TMJ (Technomedia Journal) Vol. 5 No. 1 Agustus 2020*, p. 40, 2021.

[8] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, "Determinants of Lecturer Performance to Enhance Accreditation in Higher Education," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 2020, pp. 1–7.

[9] Z. Arifin, M. Nurtanto, A. Priatna, N. Kholifah, and M. Fawaid, "Technology Andragogy Work Content Knowledge Model as a New Framework in Vocational Education: Revised Technology Pedagogy Content Knowledge Model.," *Online Submission*, vol. 9, no. 2, pp. 786–791, 2020.

[10] D. Cahyadi, A. Faturahman, H. Haryani, and E. Dolan, "BCS: Blockchain Smart Curriculum System for Verification Student Accreditation," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 65–83, 2021.

[11] Y. Durachman, A. S. Bein, E. P. Harahap, T. Ramadhan, and F. P. Oganda, "Technological and Islamic environments: Selection from Literature Review Resources," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 37–47, 2021.

[12] D. Apriani, A. Williams, U. Rahardja, A. Khoirunisa, and S. Avionita, "The Use of Science Technology In Islamic Practices and Rules In The Past Now and The Future," *International Journal of Cyber and IT Service Management*, vol. 1, no. 1, pp. 48–64, 2021.

[13] U. Rahardja, I. Handayani, N. Lutfiani, and F. P. Oganda, "An Interactive Content Media on Information System iLearning+," *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, vol. 14, no. 1, pp. 57–68, 2020.

[14] I. Rodero and M. Parashar, "Data Cyberinfrastructure for End-to-End Science," *IEEE Annals of the History of Computing*, vol. 22, no. 05, pp. 60–71, 2020.

[15] N. F. Rozy, R. Ramadhiansya, P. A. Sunarya, and U. Rahardja, "Performance Comparison Routing Protocol AODV, DSDV, and AOMDV with Video Streaming in Manet," *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*, 2019, doi: 10.1109/CITSM47753.2019.8965386.

[16] M. Prawira, H. T. Sukmana, V. Amrizal, and U. Rahardja, "A Prototype of Android-Based Emergency Management Application," *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*, 2019, doi: 10.1109/CITSM47753.2019.8965337.