International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 111-114
Published Online November 2022 in IJEAST (http://www.ijeast.com)

BLOCKCHAIN SECURITY TO PREVENT CYBER THREATS IN SMART ELECTRIC POWER SYSTEMS

Satyajit Panigrahy
Department of Electrical and Electronics Engineering
National Institute of Technology, Rourkela, Odisha

Smrutirekha Panda
Department of Electrical Engineering
Government College of Engineering, Keonjhar, Odisha

Abstract: **Over the past few years, using blockchain technology as one of the new approaches to improve the physical and cyber security of the power system has gained relevance. Blockchain can also be used to increase social welfare and give customers access to renewable energy. The next generation of power grid infrastructure, known as the Smart Power Grid, uses smart ICT (Information Communication Technology) to improve existing grid systems. It was created to overcome the drawbacks of one-way existing grid systems. With the demand for renewable energy sources, the Smart grid is anticipated to increase future power systems' efficiency and reliability significantly. Cybersecurity for the Smart Power Grid is becoming a significant issue. Since cyber-attacks by malevolent hackers can harm energy data and result in the leakage of personal information from grid members, they can cause serious incidents like massive outages and the destruction of power network infrastructure. Therefore, we will propose a secure smart energy management system built on the blockchain to fix this problem. The blockchain is a distributed data processing technology that allows for the distribution and storing of data by all network participants. By integrating blockchain technology into the Smart Grid, energy data may be managed more securely. Additionally, this will help the future growth of the smart energy sector.**

Keywords: **Smart Power System, Blockchain System, Cyber-attacks**, **Threat Prevention**

I. INTRODUCTION

The world has seen widespread blackouts for a number of years, and the harm they inflicted has heightened people's interest in effective energy resource management. These days, many nations' energy policies are being driven by smart power systems. The development of intelligent energy networks has become the main focus of global competition in the area of economic energy efficiency. Energy security, economic expansion, and environmental sustainability are the three main goals for adopting smart power systems.

Smart Grid cyber security threats can arise from various sources, including cybercrime, hacking, cyber war, etc. To mitigate cybersecurity threats, utility firms must communicate and coordinate the exchange of cybersecurity information, such as intelligence and vulnerabilities, with governmental agencies and, most likely, the public [1]. Potential assaults on Smart Power Grid communication can be avoided by recognizing the number of attacks, four of which have already been recognized. A device attack, a data attack (attempts to maliciously insert, alter, or delete data or control commands in network traffic to mislead the Smart Grid and cause it to take incorrect actions), a privacy attack (aims to learn user's private information by analyzing electricity usage data), and a network availability attack are examples of these [2].

II. BLOCKCHAIN: FEATURES AND WORKING PRINCIPLES

Blockchain technology generates a data format with intrinsic security properties. It is founded on cryptography, decentralization, and consensus concepts that enable trust in transitions. Most blockchains or distributed ledger technology (DLT) arrange data into blocks, each containing a transaction or set of transactions. Each new block in a cryptographic chain connects to all the blocks before it, making it nearly impossible to tamper with. A consensus process validates and agrees on all transactions within the blocks, ensuring that each transaction is truthful and correct [3].

A smart grid is made to solve all potential issues with electricity supply. An SM is installed at every home to collect data on power usage in close to real-time, which utilities may use to deliver better smart home services and achieve optimal scheduling in the smart grid. Blockchain technology provides decentralization by allowing members

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 111-114
Published Online November 2022 in IJEAST (http://www.ijeast.com)

of a dispersed network to participate. There is no single point of failure, and a single user cannot alter the transaction record. However, blockchain technology has significant critical security differences [3].

Blockchain-based systems combine cryptography, public critical infrastructure, and economic modeling to accomplish distributed database synchronization through peer-to-peer networking and decentralized consensus. The blockchain is essentially a distributed data structure referred to as a "distributed ledger" due to its utility in documenting transactions within a network.

III. SMART POWER SYSTEM

Current power systems typically create more energy than is required. Because it is impossible to estimate electric power consumer demand in real-time, surplus energy is produced so that electric power can be secured in advance if more electric power is needed than planned. Such a system necessitates fuel for power generation and more power plants, resulting in increased building costs. Furthermore, unused electric power diminishes energy efficiency while increasing pollution caused by the combustion of fossil fuels. Using smart information and communication technologies in the existing grid, the Smart Power system improves "situational awareness" about the state of the grid. In other words, it is a system that can intelligently maximize energy efficiency by transmitting real-time data in both directions between the power source and the user [4].

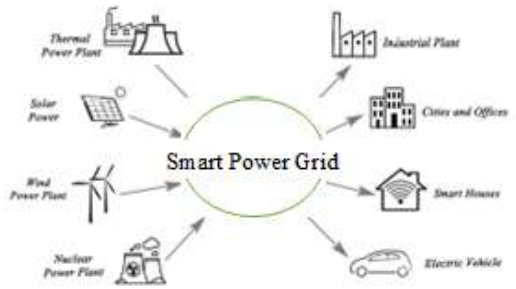

Fig 1. Smart Power Grid in industry 4.0

IV. SECURITY ISSUES OF SMART POWER SYSTEM

By seamlessly integrating high-speed metering and two-way networks into millions of power equipment, the smart Power System, which blends ICT with existing power grids, intends to develop a dynamic, interactive infrastructure with new energy management capabilities. Smart grids, on the other hand, are exposed to the potential dangers connected with communication and networking systems. In fact, the ultimate goal of the Smart Power System is to create a dependable, safe, and optimal power system, yet this goal can compromise the power system's functioning. In this section, we will examine numerous hazards that may develop in the Smart Power System, such as cyber-attack risks and the need for a solution to supplement them [5, 6].

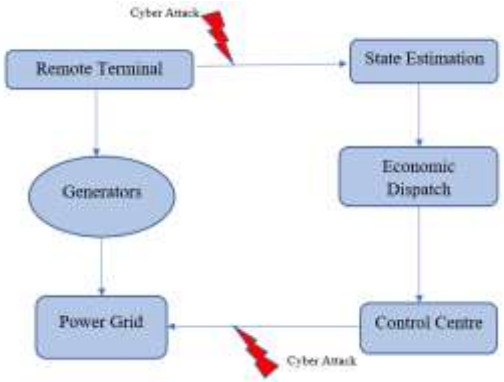

Fig 2. Cyber-attacks on Power Grid

V. CYBER SECURITY THREATS IN POWER SYSTEMS

Understanding the potential vulnerability threats in the smart power system is critical. The risk assessment approach that offers a foundation for exploiting probable entry points that are vulnerable to malicious assaults has been discussed in this section [7]. It has also been emphasized how these assaults enable an adversary to perform undesirable activities, affecting the entire smart grid system.

A. Risk Inspection and Attenuation

Risk is the possibility of an unfavorable outcome due to internal or external variables, as indicated by the likelihood of occurrence and the related consequence. Simply put, the risk is the combination of the possibility of an assault, various actions that an opponent may take, and the consequences of those actions. The initial stage in risk assessment is to identify cyber security assets, including hardware devices, network settings, software schemes, and communication protocols. Then, several testing methodologies should be implemented to check for any vulnerabilities in the existing power system.

B. Probable Attack Points and Adversary Action

An intelligent grid cyberinfrastructure must be designed to be immune to cyberspace intrusion. This is only possible if the potential access points through which an adversary can enter the system are identified. A legacy system is susceptible because many devices and apps lack built-in security features. Furthermore, for a system with such a vast number of electrical and electronic connections and powerful communication channels, making the complete innovative power system cyber-attack resistant is quite challenging [8]. However, analyzing the many attack points may assist us in planning and developing system designs and protocols that would make the smart grid attack-resistant [7, 8].

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 111-114
Published Online November 2022 in IJEAST (http://www.ijeast.com)

VI. SOLUTION: BLOCKCHAIN-BASED SECURE SMART ENERGY MANAGEMENT SYSTEM

Smart Power relies significantly on information networking. Thus, cyber-attacks have the potential to leak or change all information, from user basic information on Smart Power Systems to energy generation among prosumers. To avoid the damage caused by information leakage on the Smart Grid, a system for securely storing and transferring all information generated and exchanged on the Smart Grid is required.

In the realm of information security, numerous technologies are used, and security technologies are applied in the Smart Grid. However, the concept of a prosumer, who can deal with both energy production and trade, has resulted in the necessity for a secure energy trading system. To safely control all operations on the Smart Power System, we will present a secure smart energy management system based on blockchain technology [9].

A. Public Blockchain Security

Public blockchain networks are open to everyone, and users can remain anonymous. Using internet-connected devices, a public blockchain obtains consensus and verifies transactions. Except for public keys, this type of network has few restrictions on identity and access. The most well-known public blockchain is probably Bitcoin, which achieves agreement through "mining." [4, 10]

B. Private Blockchain Security

Private blockchains frequently let only validated, and known organizations join and use identification to verify membership and access privileges. In a permissioned network, a private blockchain gains consensus using a mechanism known as "selective endorsement," in which identified users validate transactions [11]. Together, the organizations form a private, members-only "business network," with the transaction ledger accessible only to members with certain access and permissions. For this type of network, more identification and access requirements are required [12].

VII. BUILDING BLOCKCHAIN-BASED SECURITY AROUND POWER GRIDS

It is essential to consider security at every level of the technology stack when creating a safe blockchain application and how to manage network governance and permissions [13]. Standard security measures and blockchain-specific security measures are included in a system's comprehensive security plan [14]. The following are a few security measures specific to corporate blockchain platforms [4, 13].

- Control over identification and access
- Control over critical persons
- Data protection
- Communication that is secure and safe
- Safety of smart contracts
- Approving the transaction

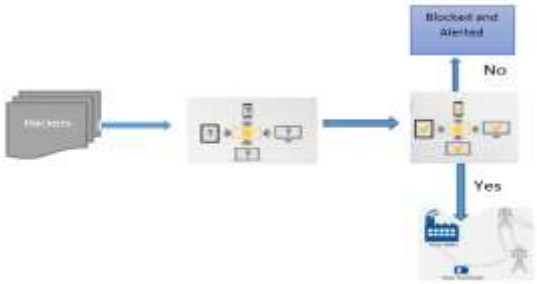

Fig 3. Blockchain-based Security Framework

VIII. BLOCKCHAIN SECURITY TIPS AND BEST PRACTICES

When we are developing a blockchain-based security solution, consider the following perspectives to better plan and execution it well [15, 16].

- What is the structure of the participating companies or members' governing bodies?
- Which information will be recorded in each block?
- What laws and regulations apply in this situation?
- How are identity details managed? Are block payloads encrypted? How are keys controlled and removed?
- What is the blockchain participants' disaster recovery strategy?
- What level of security must blockchain clients maintain to participate?
- What is the reasoning behind the resolution of blockchain block collisions?
- Ensure a private blockchain is established and deployed on a reliable, secure system to avoid vulnerabilities.

IX. CONCLUSION

Power grids are at the heart of the modern business ecosystem. Securing power grids is essential for future growth, industrialization, and development, as everything runs with power. So, ensuring our systems with blockchain-based security systems is necessary to avoid modern-day cyber-attacks. This study highlights the framework and the procedures for a successful blockchain-based model to secure our power grids. To implement a blockchain solution security model, this risk model may handle all commercial, governance, technology, and procedural issues. Future researchers are advised to create the next stage of risk assessment for the blockchain solution and create a threat model.

Acknowledgment

I thank my mentor and Associate, Prof. Balaram Das, for his guidance and input in completing this paper.

X. REFERENCES

[1]. Kim, S. M., Lee, T., Kim, S., Park, L. W., & Park, S. (2019). Security issues on smart grid and blockchain-based secure smart energy management system. In MATEC Web of Conferences (Vol. 260, p. 01001). EDP Sciences.

[2]. Ansari, M. F., Sharma, P. K., & Dash, B. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. Prevention.

[3]. Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE transactions on Industrial informatics, 7(4), 529-539.

[4]. IBM. (n.d.). What is Blockchain Security? IBM. Retrieved December 9, 2022, from https://www.ibm.com/topics/blockchain-security

[5]. Mo, Y., Kim, T. H. J., Brancik, K., Dickinson, D., Lee, H., Perrig, A., & Sinopoli, B. (2011). Cyber–physical security of a smart grid infrastructure. Proceedings of the IEEE, 100(1), 195-209.

[6]. Wang, W., & Lu, Z. (2013). Cyber security in the smart grid: Survey and challenges. Computer networks, 57(5), 1344-1371.

[7]. Sharma, P., Dash, B., & Ansari, M. F. (2022). Anti-phishing techniques–a review of Cyber Defense Mechanisms.

[8]. LeMay, M., Nelli, R., Gross, G., & Gunter, C. A. (2008, January). An integrated architecture for demand response communications and control. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 174-174). IEEE.

[9]. Framework, N. I. S. T. (2010). Roadmap for smart grid interoperability standards. National Institute of Standards and Technology, 26.

[10]. Dash, B., & Sharma, P. (2022). Role of Artificial Intelligence in Smart Cities for Information Gathering and Dissemination (A Review). Academic Journal of Research and Scientific Publishing| Vol, 4(39).

[11]. Liu, J., Xiao, Y., Li, S., Liang, W., & Chen, C. P. (2012). Cyber security and privacy issues in smart grids. IEEE Communications surveys & tutorials, 14(4), 981-997.

[12]. Dyrud, M. A. (2000). The third wave: A position paper. Business Communication Quarterly, 63(3), 81-93.

[13]. Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.

[14]. Dash, B., Ansari, M. F., Sharma, P., & Ali, A. (2022). THREATS AND OPPORTUNITIES WITH AI-BASED CYBER SECURITY INTRUSION DETECTION: AReview. International Journal of Software Engineering & Applications, 13(5), 13-21.

[15]. Chatterjee, K., Padmini, V., & Khaparde, S. A. (2017, July). Review of cyber attacks on power system operations. In 2017 IEEE Region 10 Symposium (TENSYMP) (pp. 1-6). IEEE.

[16]. Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Communications Magazine, 56(7), 82-88.