Security Issues on Smart Grid and Blockchain-based Secure Smart Energy Management System

Seung Min Kim[1], Tacklim Lee[1], Seunghwan Kim[1], Lee Won Park[2] and Sehyun Park[1]

[1]*School of Electrical and Electronics Engineering, College of ICT Engineering, Chung-Ang University, Seoul 06974, Korea*

[2]*Department of Convergence Security, Chung-Ang University, Seoul 06974, Korea*

Abstract. The Smart Grid has emerged to address the shortcomings of one-way existing grid systems, and is the next generation power grid infrastructure that applies smart ICT (Information Communication Technology) to existing grid. The Smart Grid is expected to greatly improve the efficiency and reliability of future power systems with the demand for renewable energy resources. However, because major power facilities are interconnected through communication networks, Smart Grid's cyber security is becoming an important issue. Cyber-attacks by malicious intruders can lead to serious incidents such as massive outages and the destruction of power network infrastructure, since the cyber-attacks can damage energy data, starting with personal information leakage from grid members. Therefore, as a solution to this issue we will suggest a secure smart energy management system based on the blockchain. The blockchain is a distributed data processing technology in which all users participating in the network distribute and store data. Applying blockchain technology to the Smart Grid will enable more secure management of energy data, and furthermore, it will contribute to the development of the future smart energy industry in the future.

1 Introduction

As a result of the large-scale blackout in the world for many years and the damages caused by them, interests surrounding efficient management of energy resources to overcome the power shortage has increased. In addition, it is necessary to reduce environmental pollution caused by the use and depletion of limited fossil fuels such as petroleum and coal. In addition, a system for efficient use and management of renewable energy such as wind and solar power generation is needed. The Smart Grid, which is an infrastructure that minimizes various damages while maximizing energy efficiency based on problems such as power grid paralysis, unbalanced supply/demand of energy resources, environmental pollution, and use of renewable energy, becomes an issue.

The Smart Grid, which emerged for efficient and reliable energy management, is the next generation power grid infrastructure, also known as the intelligent grid. The Smart Grid is an infrastructure for automatic control, high power conversion, optimized energy demand management, and renewable energy management technology that uses smart ICT(Information Communication Technology) to power grid in order to solve the disadvantages of existing unidirectional grid system[1, 2]. The Smart Grid has the advantage that it can work as an optimal energy management system to exchange information in real time by connecting the electricity production and distribution facilities and power consumers to the network. However, since there are security threats to energy data generated by grid members and processes, and the consequences of these threats are very lethal, efforts are needed to identify and resolve them.

Therefore, we propose a secure smart energy management solution using blockchain technology. The blockchain is a distributed data processing technology in which all users participating in a network distribute and store data[3]. The blockchain is a kind of database in which data is encrypted with a hash and stored in a block, which is then connected to a previous block in a chain form. Therefore, modifying the contents of the block are difficult because all nodes of the blockchain must be modified[4]. We will build a secure blockchain-based smart energy management system using such reliability of blockchain. In this paper, we will propose this system which will be an outline of the system to be constructed in the future.

The composition of this paper is as follows. In Section 2, we will understand the Smart Grid, the next generation power grid infrastructure, and describe the characteristics of the Smart Grid by comparing it with the existing grid. In Section 3, we discuss the various threats that can occur on the Smart Grid, and explain the risks involved in the cyber-attacks that have taken place in the Smart Grid and the need to strengthen cyber security in the Smart Grid. In Section 4, we discuss the blockchain technology and the blockchain-based system that we will propose. Finally, in Section 5 we briefly summarize the content of this paper and explain our future work.

2 Smart grid

Current power systems generally produce more than expected demand. Since it is difficult to forecast the electric power consumer demand in real time, surplus energy is produced so that electric power can be secured in advance in case more electric power is used than expected. Such a system requires not only fuel for producing power, but also additional power plants, which leads to higher construction costs. Additionally, surplus electric power which is often discarded, reduces energy efficiency while increasing environmental pollution caused by burning fossil fuels. In addition, as fossil fuels become depleted, new ways of generating electricity, transformed from the renewable energy such as wind and solar power, have been developed. As a result, a new energy platform is required to efficiently manage and real-time monitoring of various types of electric energy.

2.1 Existing grid system

Since the first grid was installed in 1886, the number of power plants has risen as the demand for electrical energy has increased from the 1970s to the 1990s. This development can be seen as a result of rapid urbanization and infrastructure development around the world. The existing grid system has a strict hierarchy with power plans at the top, as shown in the picture on the left of Figure 1, to deliver electricity to each consumer at the bottom[1]. The system uses fossil fuels to generate power centrally at the power plant, where electrical energy and data flow occur in one-way. Thus, the existing grid system cannot collect and interpret real-time data on the services offered to customers and can be viewed as a huge waste of power loss and surplus power due to the hierarchy.

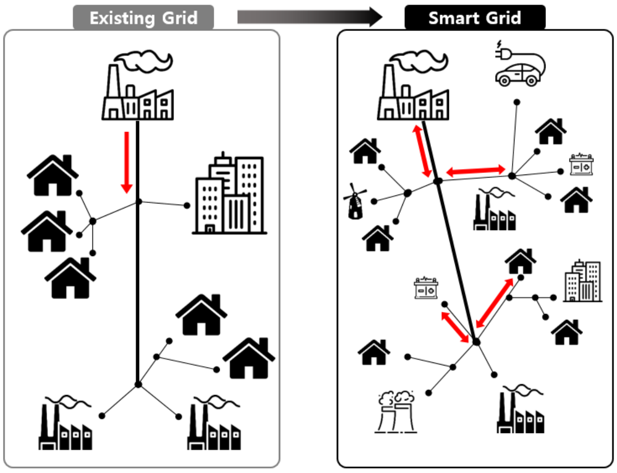

Figure 1. Change from existing grid to the Smart Grid. Smart Grid involves distributed generation, information networks, and system coordination.

2.2 Smart Grid

The Smart Grid is a compound word "Smart" plus "Grid" which means electric grid, transmission line network, substation, transformer, etc. The Smart Grid provides better "situational awareness" in relation to the state of the grid, using smart information and communication technologies in the existing grid[5]. In other words, it is a system that can intelligently maximize energy efficiency by exchanging real-time information in two-ways by the power supplier and the consumer. While the existing grid was provided to consumers as a one-way route to produce, distribute and sell electricity, the Smart Grid can exchange necessary information with each other in real-time by connecting the electricity production and distribution facilities and consumers to the network, and has the potential to provide optimized energy management[6]. A comparison of the characteristics of the existing grid and the Smart Grid is presented in Table 1.

Table 1. The Smart Grid compared with the existing grid[1]

Existing Grid	Smart Grid
Electromechanical	Digital
One-Way Communication	Two-Way Communication
Centralized Generation	Distributed Generation
Hierarchical	Network
Few Sensors	Sensors Throughout
Blind	Self-Monitoring
Manual Restoration	Self-Healing
Failures and Blackouts	Adaptive and Islanding
Manual Check/Test	Remote Check/Test
Limited Control	Pervasive Control
Few Customer Choices	Many Customer Choices

The Smart Grid can once again be defined as a system that realizes two-way secure system by integrating information from electricity creation, transmission, substation, distribution and consumption through cyber security communication technology and computer intelligence using ICT[7]. As a result, users within the Smart Grid can save energy and reduce their usage fees while increasing the reliability, efficiency, robustness and transparency of their energy management systems. Through this, the Smart Grid will be able to not only solve problems at a city or national level, but also limit the use of fossil resources, efficiently use renewable energy, and reduce environmental pollution, which are tasks to be solved globally.

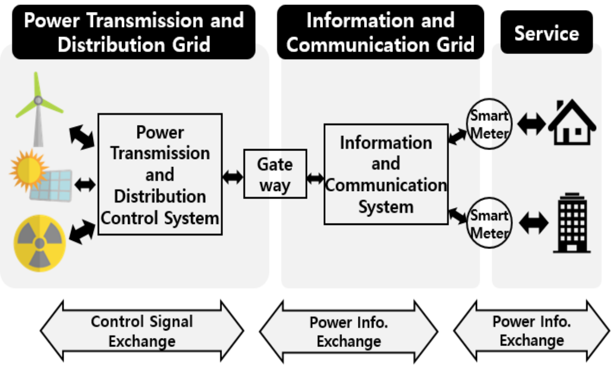
Power Transmission and Distribution Grid
Information and Communication Grid
Service
Power Transmission and Distribution Control System
Gate way
Information and Communication System
Smart Meter
Smart Meter
Control Signal Exchange
Power Info. Exchange
Power Info. Exchange

Figure 2. Smart Grid Structure

3 Security issues of smart grid

The Smart Grid, which combines ICT with existing power grids, aims to build a dynamic, interactive infrastructure with new energy management capabilities by seamlessly integrating high-speed metering and two-way networks into millions of power equipment[8, 9]. But smart grids, which rely heavily on information networking, are vulnerable to the potential threats associated with communication and networking systems. In fact, the ultimate goal of the Smart Grid is to build a reliable, safe and optimized power system, but this goal can ironically jeopardize the operation of the power system. In this section, we will look at the various threats that may arise in the Smart Grid, including the risks of cyber-attack and the need for a solution to complement them.

3.1 Existing grid system

Threats refer to various forms of behaviour that can be countered by systems either artificially or by natural means[10]. The Smart Grid architecture and infrastructure face numerous security threats and challenges such as theft, cyberattacks, terrorism, and natural disasters and so on[11]. If the Smart Grid is paralyzed by these threats, the possible outcomes are as follows: power system blackouts (small and large outages), Smart Grid IT infrastructure failures, false visualization of the actual system's condition, cascade failures, damaged consumer devices, energy market chaos, endangered human safety, etc.

Previously, various security threats and problems of Smart Grid have been researched. The threats that could damage the Smart Grid and the problems organized through previous studies are as follows[11]: theft, physical components damage, malware propagation in the cyber systems, instantaneous system malfunctioning; distributed control devices vulnerability; lack of physical protection against natural or environmental disasters such as floods, earthquakes, fire outbreaks, tsunamis, explosions, landslides, dangerous radiation leaks, pollutions, dust corrosions; inadequate control mechanisms in the conventional systems which failed to account for cyber threats; trade-off between security provisions and performance of the systems; aging of infrastructure especially those installations that were made several decades ago; industrial bottlenecks players complexities, etc.

3.2 Cyber-attacks in smart grid and risk[12]

Joe Weiss, a control system security expert, said that at least 170 cyber-related incidents have caused power outages, three of which are major outages (in 2011). In this part, we will explain the major cyber-attack cases and risks that have occurred on the Smart Grid.

3.2.1 Stuxnet

The most well-known attack by Stuxnet occurred in July 2010. Stuxnet is a malicious code that aims to reprogram certain types of industrial control systems and hide changes. This attack proved that cyber-attacks against critical infrastructures can actually be performed.

3.2.2 Night dragon

The Night Dragon, which supposedly originated from China in November 2009 to target oil and electric power companies, is a malicious code that tries to collect sensitive information related to competition of industry. This attack reminded the dangers of data and intellectual property theft in certain areas.

3.2.3 Power outage caused by hackers

In January 2008, a hacker attacked a computer system and caused a power outage. This attack did not affect many areas, but it caused a suspicion that a power outage could occur due to hacking.

3.2.4 The oil gas industry attack

In 2003, the Ohio State Nuclear Power Plant entered the computer network and became a paralysis of the safety monitoring system for about five hours. The fact that the factory was offline did not cause any harm, but it proved that outsiders could attack the control system maliciously.

4 Solution: Blockchain-based Secure Smart Energy Management System

Smart Grid is heavily reliant on information networking. Thus, cyber-attacks can cause all information, from user basic information, on Smart Grid to energy generation and usage information, and energy trading information among prosumers, to be leaked or changed all together. In order to prevent the damage caused by the leakage of information on the Smart Grid, a system for securely storing and communicating all information generated and exchanged on the Smart Grid is needed.

There are various technologies used in the field of information security, and security technologies are used in the Smart Grid. However, the concept of a prosumer(prosumer + consumer)[13], which can deal with both energy production and trade, has led to the need for a safe system for safe energy trading. We will propose a secure smart energy management system using blockchain technology to safely manage all activities on the Smart Grid.

4.1 Blockchain Technology

The blockchain is a distributed transaction and data management technology[14] that was first developed in 2008 by Nakamoto Satoshi for bitcoin[15] decryption while presenting bitcoin. In Nakamoto's paper, blockchain has received the greatest attention as a distributed transaction ledger that stores the creation of encrypted bitcoin and transaction information without a central organization such as a bank, and many studies have been applied to various fields. The precise concept of a blockchain is a distributed data processing technique in which all users participating in the network distribute and store all data so that the intermediate third party is no longer needed[3].

As shown in Figure 3, a blockchain is a form in which data is encrypted with a hash with the data of the previous block (node), stored in a block, and connected in a chain form. Therefore, it is very difficult to change the data because the previous nodes must be modified in order to change the contents in the block[4]. In addition, data for all transactions completed in the blockchain is transparent, because all users share and use data anonymously, and all nodes are connected via job credentials, making them more secure than other centralized systems.

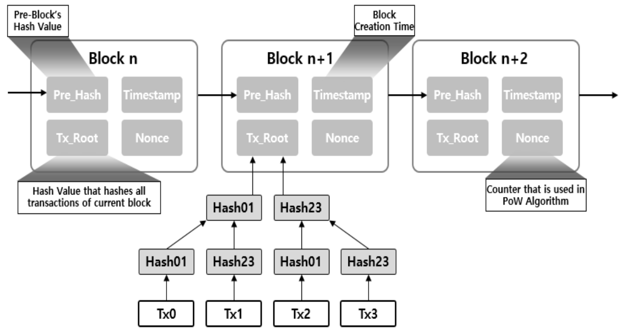

Figure 3. Blockchain - Information Recording Structure

4.2 Our solution

In this paper, we propose a secure smart energy management system based on the blockchain, which is the final goal of this paper, and explain the overall flow of the system and its expected effects.

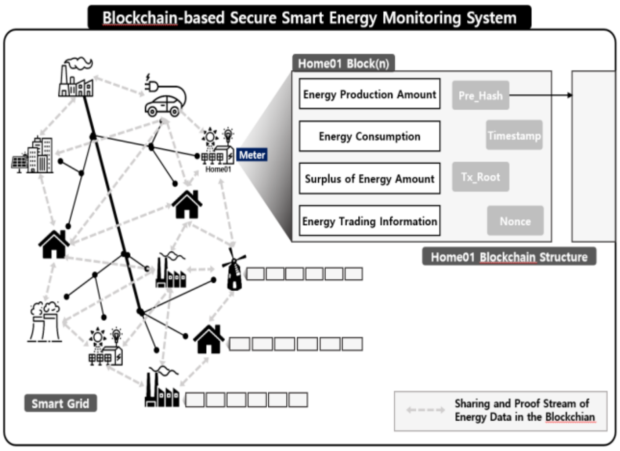
Blockchain-based Secure Smart Energy Monitoring System
Home01 Block(n)
Energy Production Amount
Pre_Hash
Energy Consumption
Timestamp
Surplus of Energy Amount
Tx_Root
Energy Trading Information
Nonce
Meter
Home01
Home01 Blockchain Structure
Smart Grid
Sharing and Proof Stream of Energy Data in the Blockchian

Figure 4. Visualization of Blockchain-based Secure Smart Energy Monitoring System

The Smart Grid will also produce and supply electricity from power plants, but each house or building will have its own solar panels installed to produce electricity. Therefore, the system will make proposals on the assumption that each household or building will voluntarily produce electricity. As shown in Figure 4, all members of the Smart Grid, such as power plants, renewable energy power plants, homes, buildings and factories, share real-time energy data in a two-way method. In the process, cyber-attacks against data may occur. Therefore, these data are hashed and encrypted in a block, stored, and connected to a blockchain in real-time to construct a database.

Let's look at the case of Home01, which produces its own power through solar panels. Because it produces its own power, the block will contain energy production, and information on energy usage, surplus energy (energy production minus energy usage) is stored. Also, in the future Smart Grid, energy transaction information is also stored because prosumers in the same grid will buy and sell energy according to their demand. This information is stored in real-time so that the connected blockchain share and prove the members of the same grid network and enhance the safety of the data.

In this system, all the energy data generated in real time in the Smart Grid is encrypted and recorded in the block, and stored in the chain, so that it is impossible to forge and steal the data. Therefore, it will be a safer and more reliable system than existing data storage systems. In addition, it is easy to grasp the amount of energy generation for a certain period of time, the amount of self-production of buildings and buildings, and the amount of usage in an organization (e.g. government) that manages a Smart Grid because users can share data among users in the same grid network. Therefore, it is easy to predict the energy production and consumption patterns of the grid members by analysing such data, and it is possible to provide efficient energy demand forecast management service. From a business point of view, real-time energy demand forecasting is possible, so it is easy for companies and governments to decide whether to invest in the energy industry in the future.

5 Conclusion

In this paper, we reviewed the Smart Grid in general and summarized various threats and cyber-attacks that may occur on the Smart Grid. We knew that if a cyber-attack occurred on the smart grid, the risk would be quite high. Therefore, in this paper, we propose a system that can make smart energy management more secure for cyber-attack in the future when smart grid is actively applied. This system can securely store and share all energy data on the Smart Grid using blockchain that has both transparency and reliability of the data. This system will not only store energy data safely, but will also be able to utilize energy data efficiently. Therefore, it is expected to contribute greatly to the development of the energy industry on the Smart Grid in the future.

In the future, we will define the detailed architecture of a secure smart energy management system based on the blockchain. After the architecture is completed, IoT devices will be used to collect energy data which will then be written to the blockchain to build our own grid. Then we will simulate whether the data in the block can be shared on the same grid and utilized through analysis. If these processes are successfully completed, we will be able to apply our complete system to the actual Smart Grid.

Acknowledgement

This work was supported by the Korea Institute of Energy Technology Evaluation and Planning(KETEP) and the Ministry of Trade, Industry & Energy(MOTIE) of the Republic of Korea (No. 20172010000470), and this research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2014-1-00636) supervised by the IITP(Institute for Information & communications Technology Promotion), and this work was supported by the Human Resources Development(No.20174030201810) of the Korea Institute of Energy Technology Evaluation and Planning(KETEP) grant funded by the Korea government Ministry of Trade, Industry and Energy.

References

1. H. Farhangis, IEEE Power and Energy Magazine, **8,** 18 (2010)
2. V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati and G. P. Hanckes, IEEE Transactions on Industrial Informatics, **7,** 529 (2011)
3. M. Swans, *Blockchain: Blueprint for a new economy*, (2015)
4. C. Burger, A. Kuhlmann, P. Richard and J. Weinmanns, DENA German Energy Agency, (2016)
5. Y. Mo, T. H. J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig and B. Sinopolis, Proceedings of the IEEE, **100,** 195 (2012)
6. R. K. Pandey and M. Misras, IEEE, 1 (2016)
7. H. GHARAVI and R. GHAFURIANs, Proceedings of the IEEE, **99,** (2011)
8. W. Wang and Z. Lus, Computer Networks, **57,** 1344 (2013)
9. M. LeMay, R. Nelli, G. Gross and C. A. Gunters, IEEE, 174 (2008)
10. J. Mendels, e-mentor, 55 (2017)
11. A. O. Otuoze, M. W. Mustafa and R. M. Lariks, Journal of Electrical Systems and Information Technology, (2018)
12. M. B. Line, I. A. Tøndel and M. G. Jaatuns, 1 (2011)
13. A. Tofflers, *The third wave*, (1989)
14. J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolanders, PloS one, **11,** e0163477 (2016)
15. S. Nakamotos, (2008)