Securing an Event-Based Smart Meter System to Prevent Pricing Cyberattack: A Preliminary Research

Desti Nirwana Mozef[1], Fadhil Hidayat[2]
{destimozef@students.itb.ac.id[1]}

Bandung Institute of Technology[1,2]

Abstract. Being a part of the smart grid, a smart meter is a device that is widely used nowadays because it is expected to improve the efficiency of the current electricity network by using advanced digital information and communication technology. One of the advantages of using the smart meter is it can simplify the billing process. However, because the smart meter system must be connected to intranet and extranet networks, it becomes vulnerable to several security and privacy threats. One of the major concerns is pricing cyber-attack, which happens when energy consumption data becomes the target of an attack because this can affect the amount of billing that must be paid by costumers. There are already several studies that discussed securing the smart grid system using various methods but those are still computationally complex and only implemented on time-based type smart meters. The aim of this paper is to present preliminary research on securing an event-based smart meter system from a pricing cyber-attack.

Keywords: Smart grid, Smart meter, Pricing cyberattack

1 Introduction

One of the problems in urban areas is decent housing that is also safe and comfortable. A safe and comfortable home is a house that can make it easier for the homeowners to carry out their daily activities and that can make it possible for homeowners to control and monitor the house and the devices inside from anywhere so that homeowners will feel safe when leaving home. Unfortunately, conventional houses that are inhabited by most people do not allow those services. In such houses, electronic devices are controlled manually.

However, along with the development of technology, a concept called the internet of things (IoT) makes controlling electronic devices at home wirelessly become possible. Such a system is called a smart home. According to Satpathy [1], smart home is an intelligent system in the scope of a house that can help humans to live independently and comfortably using technological assistance in which all mechanical and digital devices are interconnected in a network that can create an interactive space. A smart home allows various services that facilitate human work such as entrance monitoring, room temperature control, electronic device control, lamp control, energy management, etc.

One of important elements in the smart home is the smart meter. Smart meters are devices that have a power sensor so that they can read and monitor the power consumption of connected electronic devices. The data that has been obtained then will be sent to a monitoring system through the cloud to be converted into cost information using wired or wireless communication. There are two ways for the smart meter to send its data, the first one is time-

MSCEIS 2019, October 12, Bandung, Indonesia

DOI 10.4108/eai.12-10-2019.2296521

based where the data is sent at each predetermined time interval. The second one is event-based where the data will be sent only if there is a trigger to the smart meter that occurs every time an activity is carried out by the homeowner.

The use of smart meter is currently increasing and has been installed in various regions throughout the world because the smart meter has many advantages offered. Based on a report from Pike Research, it is estimated that the use of smart meters has tripled from 10.3 million units in 2011 to 29.9 million units in 2017. This smart meter infrastructure, when used appropriately, can not only provide information about users' energy consumption but also can act as Automated Meter Reading (AMR) and data processing, simplify the billing process and detect energy theft [2].

However, because smart meters are used for monitoring, smart meters must be connected to intranet and extranet networks. Therefore, the devices on the smart home system can be attacked from inside and outside. The impact of attacks on the smart meter will be very severe as it brings serious privacy issues toward customers, for example, identity theft of the homeowner. That might happen because the data received and sent from or to the smart meter is the privacy of consumers. Several studies have shown that energy consumption data can reveal personal information about home residents such as lifestyle and economic status [3] ,[4] [5], [6] [7].

That energy consumption information from smart meters is used to determine pricing information. Sometimes, there are also malicious attackers who inject false energy consumption data or corrupt the meter readings to change the estimated bill that needs to be paid. To prevent this attack from happening, a secure billing system is needed on the smart meter system. Several studies have discussed the secure billing system on the smart meter using various methods.

This paper presents the literature review of the secure billing system on the smart meter to prevent pricing cyberattacks. The research aims to provide the advantages and disadvantages of each method used in previous research to find the most suitable method to use that also has been able to meet several security requirements such as confidentiality, integrity, availability, and privacy.

The structure of this paper is organized as follows. Section 2 provides related work that discussed previous studies on a secure billing system. Section 3 describes the proposed works and the procedure to select the most suitable method. Section 4 concludes the paper.

2 Review of Existing Secure Smart Meter

Based on the type of smart meter, studies that discuss security in the event-based smart meter is fewer than a time-based smart meter. One of which is a study by Simonov [8] that proposed a method to protect the information in the context of event-based energy management systems in a consumer-centered smart grid with renewable energy. The attack model for this study is the packet injection that aims to mislead the energy management system.

To securing smart meter data, there are some methods that have been discussed or performed on several previous studies such as mathematical analysis, cryptographic approach, and blockchain. Based on mathematical analysis, Han-Xiao [9] proposed a non-technical loss fraud detection (NFD) to prevent energy theft. The NFD used Lagrange polynomial interpolation model to detect the behavior of multiple compromised meters and multiple adversaries.

Based on the cryptographic approach, Wang [10] proposes an efficient privacy-preserving aggregation and billing protocol in a smart grid based on Paillier's homomorphic encryption and verifiable secret sharing, but in this scheme, the smart meter is not authenticated and also do not ensure data integrity. Gope [11] propose a privacy friendly and efficient data aggregation scheme for dynamic pricing based on billing and demand-response management in smart grids. This scheme is based on symmetric key cryptographic primitives such as hash functions, which cause very limited computational overhead and data aggregation time. Ni [12] design a dynamic billing mechanism based on individual power consumption with the verification of customers. This scheme achieves the authentication, confidentiality, and integrity of consumption reports based on Chameleon hash function, proxy re-encryption, and homomorphic authenticators. Guan [13] proposes a privacy-preserving and efficient data aggregation scheme based on the blockchain to preserve the user's privacy in the smart grid. Pseudonyms are adopted to protect the user's identities and Bloom filter is adopted for fast authentication.

3 Proposed Works

This section will explain the important aspects of smart grid systems particularly its security. In the last part of this section, there will be a comparison table based on those aspects between the previous studies and the proposed work.

3.1 Smart Meter's Type

3.1.1 Time-based

In time-based smart meters that are widely used, the energy consumption reports are carried out at certain time intervals, for example, every month or every 10 minutes. The reports will be sent by the smart meter upon regular timers by using a standard communication protocol. In other words, the smart meter will send its data in every Δt and the lowest possible Δt is one second which is assumed as real-time measurement. But this kind of smart meter is not efficient if the homeowners are away and there is no activity from the devices in the house. To overcome this problem, there is another strategy known as event-based metering.

3.1.2 Event-based

In event-based metering, the energy consumption reports only will be sent if there is an activity from the homeowners which can be identified from some criteria [14], such as a transition in power demand and there is a reading of the energy consumption. This strategy is based on the fact that most of the time, the power needed by the appliance stays constant.

3.2 Architecture for Smart Grid System

Based on a survey paper about the smart grid's architecture [15], it is said that there are several architectures available for the smart grid system.

3.2.1 Three-Layered Architecture

This architecture consists of three layers, a perception layer, a network layer and an application layer as shown in **Figure 1**.

a) Perception Layer

The main purpose of this layer is to sense and collect information in the smart grid system by using various devices such as RFID tags, cameras, WSN, GPS and M2M devices. This layer also consists of two sub-layers, a perception control sub-layer and a communication extension sub-layer. The function of the perception control sub-layer is for information acquisition, processing IoT devices, monitoring, and controlling. The function of the communication extension sub-layer is for connecting IoT devices with the network layer.

b) Network Layer

The function of the network layer is for mapping information obtained by IoT devices in the perception layer to the telecommunication protocols then the information will be transmitted to the application network.

c) Application Layer

The function of the application layer is for processing the information which is obtained from the network layer then monitoring the IoT devices and smart grid system in real-time based on that information.

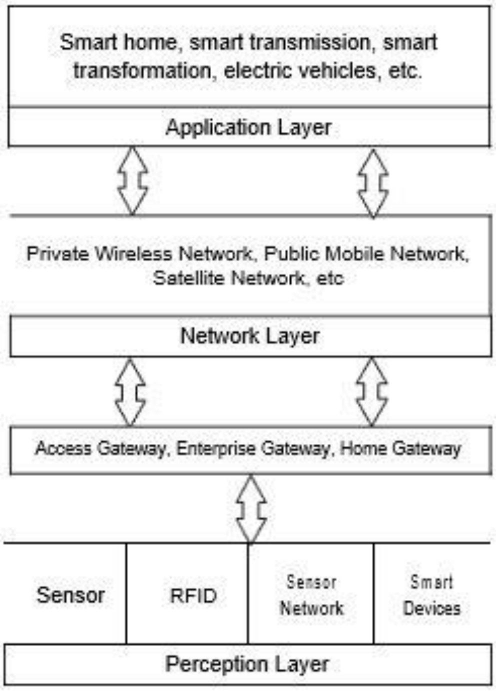
Smart home, smart transmission, smart transformation, electric vehicles, etc.
Application Layer
Private Wireless Network, Public Mobile Network, Satellite Network, etc
Network Layer
Access Gateway, Enterprise Gateway, Home Gateway
Sensor
RFID
Sensor Network
Smart Devices
Perception Layer

Fig. 1. Three-Layered Architecture

3.2.2 Four-Layered Architecture

Based on the characteristics of smart grid communication and information system, a four-layered architecture was proposed [16]. This architecture consists of a terminal layer, field network layer, remote communication layer, and master station system layer as shown in **Figure 2**. The terminal and field network layer in this architecture are similar to the perception layer in three-layered architecture, the remote communication layer is similar to the network layer, and the master station system layer is similar to the application layer.

The terminal layer consists of IoT devices which are used in various smart grid function such as remote terminal units, smart meters, information collection devices, etc. The purpose is to collect information from the IoT devices and transmit that information to the field network layer. In the field network layer, a communication network that is suitable for the IoT devices is used, it can be wired or wireless. Remote communication network layer consists of communication networks that provide connectivity to the Internet, such as 2G, 3G, LTE, and optical network. The master station system layer is the interface of the smart grid application to control and manage the information system of a smart grid.

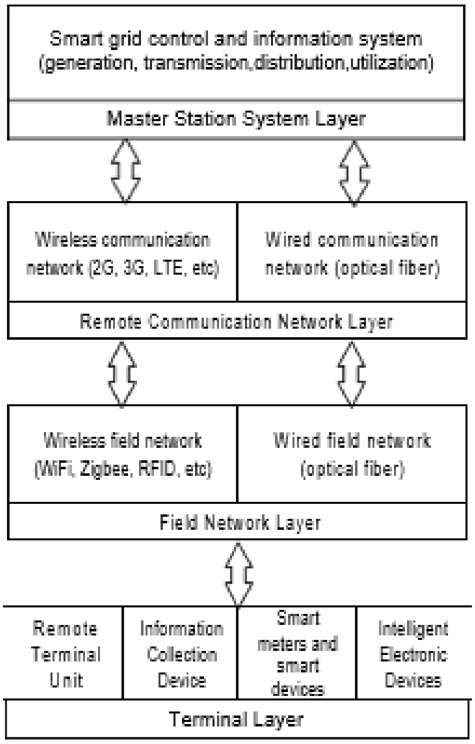
Smart grid control and information system
(generation, transmission,distribution,utilization)
Master Station System Layer
Wireless communication network (2G, 3G, LTE, etc)
Wired communication network (optical fiber)
Remote Communication Network Layer
Wireless field network (WiFi, Zigbee, RFID, etc)
Wired field network (optical fiber)
Field Network Layer
Remote Terminal Unit
Information Collection Device
Smart meters and smart devices
Intelligent Electronic Devices
Terminal Layer

Fig. 2. Four-Layered Architecture

3.3 Security on Smart Meter System

3.3.1 Security Requirement

a) Confidentiality

Ensuring that energy consumption data can remain confidential from any unauthorized third party.

b) Integrity

Ensuring that energy consumption data sent from smart meters cannot be modified by the attacker.

c) Authentication

Ensuring that energy consumption data from each customer is from legitimate customers, so it’s impossible for the operation center to receive false reports.

d) User's privacy

Ensuring that no attacker can read any customer's personal data from the smart meter.

3.3.2 Attack Model on Smart Meter System

There are several attacks that might happen to the smart meter system, but the focus of this research is a pricing cyberattack where the attacker manipulates the energy consumption pricing. To do this kind of attack, the attacker can inject false energy consumption data or corrupt the meter readings to change the estimated bill that needs to be paid. **Figure 3** shows the attack model in a smart grid architecture for the proposed system.

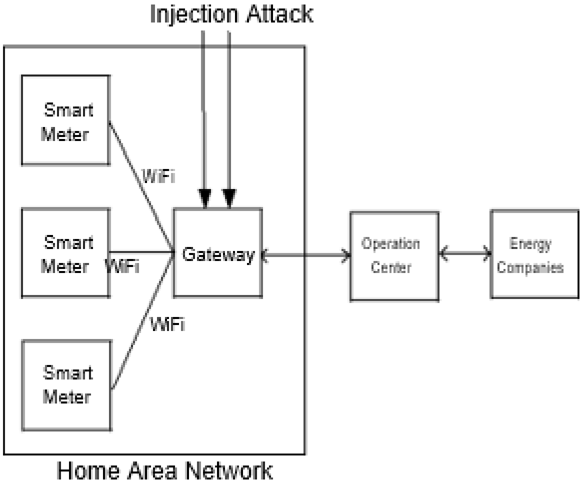

Fig. 3. Smart Grid Architecture and Attack Model

3.3.3 Security Method

As shown in **Table 1**, the most commonly used methods are cryptographic approaches such as pallier homomorphic encryption, symmetric encryption, BGN cryptosystem, and elgamal encryption. Those methods have their own advantages and disadvantages. As for pallier homomorphic encryption, fully homomorphic, and elgamal encryption, it is said that the operations are computationally expensive and may not be suitable for the resource-limited smart meters. So, to overcome that issue, research by Gope [12] proposed a computationally efficient dynamic pricing-based billing system using symmetric key cryptographic primitives such as hash functions which is suitable for the resource-constrained devices in smart grids.

Table 1. Taxonomy Methods on Previous Research.

Methods Used	
Mathematical Analysis	Nontechnical loss fraud detection (NFD) [9]

Cryptographic Approach	Linear Regression [17] Fully homomorphic technique [18] Paillier homomorphic encryption [10], [19], [20], [21], [22], [23] Verifiable secret sharing [10], [24] Symmetric cryptography [11] BGN cryptosystem [25]
Blockchain	Elgamal encryption [12], [26], [27] Pseudonym, bloom filter [14]

3.4 Research Positioning

After reviewing previous studies summarized in Section II and knowing important aspects of the smart meter system, the next step is to determine the position of the proposed work based on several aspects as in **Table 2**.

Table 2. Research Positioning.

	Ohara (2014)	Ni (2017)	Gope (2018)	Proposed (2019)
Communication	-	WiFi/Zigbee & Internet	Wifi & LTE-A	WiFi Internet
Smart meter's type	Time-based	Time-based	Time-based	Event-based
Methods	Homomorphic encryption, elgamal encryption	Chameleon hash function, proxy re-encryption, homomorphic authenticator	Lightweight symmetric-key-based cryptographic primitives	Lightweight symmetric-key-based cryptographic primitives
Attack	Injection attack	Injection attack	Replay attack, eavesdropping	Injection attack
Security Requirements	Confidentiality, integrity	Confidentiality, Integrity, Authentication,	Confidentiality, Integrity, Authentication,	Confidentiality, Integrity, Authenticati

	Ohara (2014)	Ni (2017)	Gope (2018)	Proposed (2019)
		Privacy	Privacy	on, Privacy

4 Conclusion

After reviewing various studies about the secure smart meter system as preliminary research, it can be known that there are some aspects to be considered. In the proposed work, the communication will be using WiFi to connect the smart meter to the gateway and Internet to connect the gateway to the operation center. A smart meter's type that will be used is event-based smart meter because it will be more efficient if the homeowners are often away. To secure the system, the methods that will be used is symmetric key-based cryptographic because its computationally efficient and is suitable for the resource-constrained devices in smart grids. The method will be used to secure the smart meter system from a pricing cyberattack using an injection attack.

References

[1] Satpathy, L.: Smart housing: Technology to aid aging in place. New opportunities and challenges, M.S. thesis Mississippi State Univ, Starkville. (2006)

[2] Alahakoon, D., dan Yu, X.: Smart Electricity Meter Data Intelligence for Future Energy Systems: A Survey, IEEE Transactions On Industrial Informatics, 12. (2016)

[3] Wood, G., dan Newborough, M.: Dynamic energy-consumption indicators for domestic appliances: Environment, behaviour and design, Energy Build., vol. 35, no. 8, pp. 821–841. (2003)

[4] McDaniel, P., dan McLaughlin, S.: Security and privacy challenges in the smart grid, IEEE Security Privacy Mag., vol. 7, no. 3, pp. 75–77. (2009)

[5] Quinn, E.: Privacy and the New Energy Infrastructure. [Online]. Available: http://ssrn.com/abstract=1370731. (2009)

[6] Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., dan Irwin, D.: Private memoirs of a smart meter, Proc. ACM Workshop Embedded Sens. Syst. Energy Efficiency Build. (BuildSys), Zürich, Switzerland, pp. 61–66. (2010)

[7] Kalogridis, G., Cepeda, R., Denic, S. Z., Lewis, T., dan Efthymiou, C.: ElecPrivacy: Evaluating the privacy protection of electricity management algorithms, IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 750–758. (2011)

[8] M. Simonov and G. Zanetto.: "Secured event-based smart meter," 2017 3rd International Conference on Event-Based Control, Communication and Signal Processing (EBCCSP), Funchal, pp. 1-6. (2017)

[9] W. Han and Y. Xiao.: "Nfd: Non-technical loss fraud detection in smart grid," Computers & Security, vol. 65, pp. 187-201, (2017)

[10] X.-F. Wang, Y. Mu, R.-M. Chen.: "An efficient privacy-preserving aggregation and billing protocol for smart grid", Secur. Commun. Netw., vol. 9, no. 17, pp. 4536-4547, (2016)

[11] P. Gope and B. Sikdar.: "An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-Based Billing and Demand-Response Management in Smart Grids," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3126-3135, Aug. (2018)

[12] J. Ni, K. Zhang, X. Lin and X. S. Shen.: "Balancing Security and Efficiency for Smart Metering Against Misbehaving Collectors," in IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 1225-1236, March (2019)

[13] Z. Guan et al.: "Privacy-Preserving and Efficient Aggregation Based on Blockchain for Power Grid Communications in Smart Communities," in IEEE Communications Magazine, vol. 56, no. 7, pp. 82-88, July (2018)

[14] M. de Castro Tome, P. H. J. Nardelli, H. Alves.: "Event-based electricity metering: An autonomous method to determine transmission thresholds", Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring), pp. 1-5, Jun (2018)

[15] Y. Saleem, N. Crespi, M. H. Rehmani and R. Copeland.: "Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," in IEEE Access, vol. 7, pp. 62962-63003. (2019)

[16] Y. Wang, W. M. Lin, T. Zhang, and Y. Y. Ma.: ``Research on application and security protection of Internet of Things in smart grid," in Proc. Int. Conf. Inf. Sci. Control Eng. (ICISCE),pp. 1-5. Dec (2012)

[17] S.-C. Yip, K. Wong, W.-P. Hew, M.-T. Gan, R. C.-W. Phan, and S.-W. Tan, "Detection of energy theft and defective smart meters in smart grids using linear regression," International Journal of Electrical Power & Energy Systems, vol. 91, pp. 230–240, (2017)

[18] X. Liang, X. Li, R. Lu, X. Lin and X. Shen.: "UDP: Usage-Based Dynamic Pricing with Privacy Preservation for Smart Grid," in IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 141-150, March (2013)

[19] F. Garcia, B. Jacobs.: "Privacy-friendly energy-metering via homomorphic encryption", 6th Workshop on Security and Trust Management (STM), (2010)

[20] H. Li, X. Lin, H. Yang, X. Liang, R. Lu and X. Shen.: "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2053-2064, Aug. (2014)

[21] K. Kursawe, G. Danezis, M. Kohlweiss.: Privacy-friendly aggregation for the smart-grid, [online] Available: http://research.microsoft.com/apps/pubs/?id=146092

[22] R. Lu, X. Liang, X. Li, X. Lin and X. Shen.: "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621-1631, Sept. (2012)

[23] H. J. Jo, I. S. Kim and D. H. Lee.: "Efficient and Privacy-Preserving Metering Protocols for Smart Grid Systems," in IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1732-1742, May (2016)

[24] C. Rottondi, G. Verticale, C. Krauss.: "Privacy-preserving smart metering with multiple data consumers", Comput. Netw., vol. 57, no. 7, pp. 1699-1713, May (2013)

[25] C. Fan, S. Huang and Y. Lai.: "Privacy-Enhanced Data Aggregation Scheme Against Internal Attackers in Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 666-675, Feb. (2014)

[26] K. Ohara, Y. Sakai, F. Yoshida, M. Iwamoto, K. Ohta.: "Privacy-preserving smart metering with verifiability for both billing and energy management", Proc. of AsiaPKC 2014, pp. 23-32, (2014)

[27] X. Liu, Y. Zhang, B. Wang, H. Wang.: "An anonymous data aggregation scheme for smart grid systems", Secur. Commun. Netw., vol. 7, no. 3, pp. 602-610, Mar. (2014)