ISSN 2278-3091
Volume 8, No.1.6, 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse4881.62019.pdf
https://doi.org/10.30534/ijatcse/2019/4881.62019

Cyber Vulnerabilities in Smart Grid and Safety Measures for Energy Meters in Advanced Metering System and Smart Meter Communications

Afida Ayob[1] , S. M. Salim Reza[1], Aini Hussain[1], Mohd Hanif Md Saad[1] and Nowshad Amin[2]
[1]Centre for Integrated Systems and Advanced Technology (INTEGRA), Department of Electrical, Electronics and Systems, Faculty of Engineering and Built Environment, The National University of Malaysia, 43600 UKM Bangi, Malaysia.
[2]Institute of Sustainable Energy (ISE), Universiti Tenaga Nasional, 43000 Kajang, Malaysia.
salim4419@gmail.com

ABSTRACT

A smart grid (SG) utilizes many electronic devices that can communicate within the system and remain internally connected through implementing advanced Information and Communication Technologies (ICT). This paper analyzes the complete structure of a smart grid system, implementation of technologies such as Supervisory Control and Data Acquisition (SCADA) and smart metering, as well as identifies the potential cyberthreats. As the connected devices have significant limitations in terms of resource and computational processing power, it calls for developing a lightweight safety measures for those devices which would require low processing power and can operate instantaneously without outside intervention. Based on such requirement, this paper has proposed a lightweight and easily implementable safety measure for Advanced Metering Infrastructure (AMI) using ChaCha20 encryption model. It also uses chaos based key generation as well as public key-based authentication techniques. Besides, to ensure security of the network communication, a solution has been proposed using Elliptic Curve Cryptography (ECC) in combination with Salsa20 stream cipher algorithm. Comprehensive mathematical simulations have been conducted for both methodologies to examine their effectiveness in the real world, and to analyze whether they are efficient in terms of time and processing power. It has been found out that Salsa20 is more energy-efficient encryption tool, which is also faster, making it the perfect choice for smart metering devices.

Key words : Advanced Metering Infrastructures Cybersecurity, Smart Grid, Smart Meter Communication

1. INTRODUCTION

Smart Grid (SG) is considered as a futuristic power generation and distribution system that brings together the renewable sources of power alongside the traditional power generation system. A traditional power grid system uses typical energy meters for consumers to measure the amount of electricity consumption [1]. A typical watt-hour energy meter is made with a spinning aluminum disc located on a spindle between two electromagnets, and electricity consumption is measured with the rotation speed of the disc, which is rotated using gear trains and counter mechanism [2]. A smart meter is a special type of energy meter to measure and monitor electricity consumption digitally and to communicate the data over a secured network as an IoT device. This paper limits the discussion of energy meter to the category of smart meter only, because of its increasing importance in the modern world an IoT device.

The key idea of SG is to establish a communication network of several devices from both generation and transmission side consisting thousands of consumer-level smart meters (SM) and power generation units with the facility of real-time bi-directional communication network. The structure is often referred as Advanced Metering Infrastructure (AMI) [3]. Demand response from customers received from SM are instantly communicated through the system and sent to the control center for analysis. The information is used for efficient power generation and smooth transmission, which eventually contributes significantly to the cost reduction of the operation both from utility's and customers' ends [4].

These massive grids of interconnected two-way communication networks consist of a wide array of modern technologies such as private & wide area network and including AMI. As one of the most important and basic tool of SG network, AMI performs the collection and transportation of data from the customers to utility companies, where its role is to function as a connecting gateway or bridge [5]. There can be two types of cyber-attacks on an SG, which are insider and outsider attacks. During an insider attack, the attacker penetrates the internal devices of a network and jeopardizes it with false messages. This may lead to packet dropping and communication of wrong data throughout the network. In contrast, to perform an outsider attack, the attacker does not need to enter the system, rather can perform it externally by hampering the network communication. Some traditional cryptography techniques are used to prevent such attacks such

as PKI-dependent schemes or digital signatures. However, they are expensive to implement and requires significant amount of computational resources making the system inefficient [6].

This paper has emphasized on the idea that complicated security models that require high processing and computational resources, energy and cost are not suitable for AMI, SM and SG devices. With the objective in mind, this paper has recommended a lightweight and easily implementable security model based on ChaCha20 encryption technique and compared the output with more traditional Advanced Encryption Standard (AES)-based model through mathematical simulation [7]. It is found out that ChaCha20-based encryption has performed in a more effective and feasible way in such tests, and suitable for use in any AMI-connected devices.

2 BACKGROUND DISCUSSION & REVIEW OF LITERATURE

2.1 Importance of IoT Technology in Smart Grid

SG enables continuous and reliable communication of data of different kinds of power sources including traditional and renewable ones with the help of self-driven management mechanism and modern tools ensuring better competences in terms of dependability, effectiveness and safety. One of the most crucial roles of an SG is to guarantee a match between energy supply and demand to avoid system instability due to voltage changes that might occur if an attack takes place. This is done by an operation center that calculates, controls and examines real-time energy demand using an advanced metering infrastructure (i.e. AMI) and adjusts supplies accordingly [8]. For example, if households possess a Distributed Energy Resource (DER), such as solar panel, then electricity is generated, and the generation data is forwarded to the grid operators and suppliers at regular intervals round the clock. Being able to access these detail data in real time, the grid enjoys an important benefit. Producers can forecast their customers' power consumption and produce more accurately minimizing any system loss. It is essential for the suppliers to have access to error-free consumption and production reports as they must pay a high amount of imbalance fees for variation of the actual consumption compared to supply and production [9].

2.2 Overview of Vulnerabilities and threats on smart grid system

Despite having a wide range of advantages compared to traditional grid, an SG is susceptible to cybercrime from three levels [10], and it is vital to put protection mechanisms for all three levels separately. At the first level, the electrical components and the SMs including the signals they generate and forward to the concentrator nodes are exposed to attackers due to the physical accessibility of the devices. On the second level, the signals that are generated from the SMs through the concentrator nodes and up to the data centers and various web-based applications can be hacked distantly to exercise control over the system. On the third level, the graphical user interface (GUI) and value-added-services that collects and presents all the data to the end users may also be vulnerable. One of the most vital elements in an entire smart grid system is the Supervisory Control and Data Acquisition (SCADA) systems through which an attacker may be able to penetrate the entire framework. In summary, SCADA denotes a computerized framework for collection and analysis of data in real time through various sources and sensors and utilization of that data to oversee & validate the operation of a plant or equipment [11]. In 2010, the Stuxnet malware that attacked and jeopardized more than 30,000 computers in Iran as well as a nuclear power plant was carefully designed and specifically customized to attack the SCADA network [12]. According to Dr. Avishai, CTO of AlgoSec, a prominent cybersecurity consultancy firm, one of the main drawbacks of a regular SCADA system is its incapacity to distinguish a genuine request generated by the sensors from a harmful request generated by a malware [13].

SMs, despite having protection tools and mechanisms against bodily harm through use of advanced microcontrollers, they are still exposed to risk related to electricity theft and falsified data injection attacks. Therefore, as a system-wide trusted entity, a reliable authority should be placed in the AMI system model making it responsible for producing and transmitting secret verification keys to household users and operation center in random basis using secure communication channels [14]. According to the cybersecurity specialists, it is likely to attack the SM network with a malware remotely over the internet and disrupt energy flow to the individual customers. This may even lead to terrorist attacks if it is performed in a greater scale. Cybersecurity researcher Netanel Rubin, co-founder of the security firm Vaultra, says it is possible to hack the SMs that are installed in the UK at present, with a single line of malicious code [15].

2.3 Security system for SG network

It has been pointed out by several prominent researchers that an easily implementable and less complicated security system is recommended for SG network due to limitations of resources and processing power. However, most of the methodologies that are widely practiced in the industry are more appropriate for a portion of the system rather than the entire system. For instance, a security protocol that is suitable for subsystem such as communication between smart meter (SM) and service provider (SP), may not be the most efficient one for communication between consumer and substation, and at the same time they do not guarantee systemwide

effectiveness. Besides, Advanced Encryption Standard (AES) based highly complicated security measures may not be the appropriate one to be implemented in low cost devices such smart meters [7].

Recently, several methods have been prescribed by researchers considering resource limitation of SM. An easygoing Elliptic Curve Cryptography (ECC)-based verification mechanism has been proposed in [16] known as LiSA. AES-128 has been proposed by some researchers as a dependable cryptography technique where it was suggested to convert client's data into chipper text mode before sending to server through HTTP protocol. However, it was found out that performance of such system is significantly dependent on data size as larger data size requires much higher processing time [17]. IoT devices most of the time are usually limited in terms of resource and power supply. For example, the power supply system that manages the task of distributing required power to the components and regulating the voltage from the battery of a proposed agricultural IoT device is capable of running at only 5V with a 5000 mAh Li-ion battery [18].

Shared private key and random number based minimalistic authentication mechanism has been prescribed in [19] for correspondence within supervisory node and control node. PUF and monodirectional hash function-based cryptography has also been suggested to ensure secured communication among SM and service provider [20]. Public key-based approach has been tested in [21] which ensures verification, reliability, discretion and non-denial. However, energy efficiency is not optimal for public key-based schemes.

Keeping this real-life constraint in mind, a ChaCha20 encryption-based security methodology has been developed to keep the SG network safe from external cyberattacks [22]. Developed by Daniel J Bernstein to be faster, ChaCha20 is a well-known non-complex cipher whose main advantage lies in its ARX-based (Addition, Rotation and XOR) design language that ensures speed, reduces complications and prevents from timing attack. ChaCha20 is deemed suitable for SG network mainly for its lightweight size and processing power requirement. This paper has used Chaotic map based random number generation technic because of the non-linearity characteristic of chaotic map making it difficult to crack and having good cryptographic characteristics [23].

3. METHODOLOGY

3.1 Security Scheme for Advanced Metering Infrastructures

Two main stages of the prescribed model in this paper are initialization and information exchange. Specific keys are assigned to the devices first, and the devices initiate communication in the information exchange stage upon self-authentication through exchange of keys. Once authentication is completed, they start to communicate through ChaCha20 method. The overview of the security system is depicted in Figure 1.

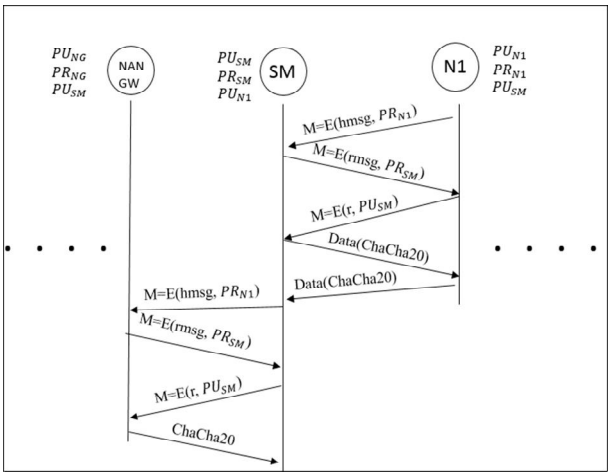

Figure 1: Overview of the Security Scheme

3.1.1 Initialization Stage

Each individual SM would perform a test in the initialization stage to check the legitimacy of connected device, which is done through the assigned public and private key denoted by PU_i and PR_i respectively. A hello message *hmsg* will be communicated from the connected devices to the nodes and SMs that are ciphered with private key PR_i. SM already has the specific assigned public key PU_i of the smart device and will be able to decode the message. It will again respond back a *rmsg* message, that is coded with PR_i. This is how both devices will be able to cross-verify themselves. Later, connected nodes will communicate the hidden value of chaotic system's parameter, *r*. From this value both the node and SM will be able to develop necessary keys to perform the ChaCha20 encryption algorithm. This is applicable for all individually paired devices within the system.

3.1.2 Information Exchange Stage

ChaCha20, which is derived from Salsa20 encryption by Daniel J Bernstein [22], has been proposed in this stage due to its high level of efficiency in terms of resource usage and very little complexities. In summary, ChaCha20 accepts plain texts (Pi_i) which are 16-words in length as inputs and processes it to produce 16-words lengthy outputs or encrypted texts (C_i). Therefore, encrypted text (Ci) = plain text (Pi) $\oplus$ ChaCha20 key stream and the decryption takes place in reverse order of encryption as plain text (Pi) = encrypted text (Ci) $\oplus$ ChaCha20 key stream. The key stream is derived from

ChaCha20 block function that initiates a few round functions based on 4*4 matrix which includes a 4-bytes counter value, eight nos 4-bytes key, four nos 4-bytes constants as well as 3 nos 4-bytes Nonce. Four 4-bytes words are computed by the algorithm in parallel.

ChaCha20, uses quarter round function to rearrange the initial blocks of 64 bytes (consisting 16 words). In each of the 16 words of a single packet, in total 20 rounds of encryption are performed that includes 10 diagonal rounds and 10 column rounds. Total four quarter rounds of computational encryptions take place on four 4bytes of words in each round:

a+ = b; d^ = a; d <<<= 16; (1)
c+ = d; b^ = c; b <<<= 12; (2)
a+ = b; d^ = a; d <<<= 8; (3)
c+ = d; b^ = c; b <<<= 7; (4)

In the above functions, module 2^{32}, XOR operation, and rotation toward larger bits are indicated by +, hat and <<<, respectively. After completion of 20 rounds, the outputs are totaled with initial input matrix. Lastly, the derived key stream is XORed with input and generates encrypted text.

3.1.3 Key Generation

To derive key for ChaCha20 encryption, this paper has considered a discrete time chaotic system that is basically a polynomial equation known as logistic map. Such logistic map is expressed by the following equation [24]:

$$X_{n+1} = rX_n(1 - X_n) \quad (5)$$

The system parameter is denoted by r and the input values range between 3.5699 to 4. In this simulation, it is assumed that, r = 3.99 and primary value, X_o = 0.6 (which always range from 0 to 1). As the requirement of ChaCha20 encryption to run, first 8 numbers of location map equation (1) will be considered for plotting the diagram. The values are as follows: 0.6, 0.958, 0.162, 0.543, 0.99, 0.038, 0.145 and 0.496.

Followed by the simulation, the values are converted into 32-bit binary through multiplication with (2^{32} - 1) equivalent decimal value and rounding to the closest number.

3.2 Security Scheme for Smart Meter Communication

To derive an efficient cryptography methodology for internal communication of Smart Metering (SM) devices, this paper has examined the effectiveness of Salsa20 method [25], which is developed with Addition, Rotation and XOR (ARX). The paper also suggests to application of additional verification process based on elliptic curve before any type of data exchange.

3.2.1 Initialization Stage

The initial verification of SM and other network-connected devices will take place with the help of ECC [26]. For this verification, each of the network-connected devices (i) will use a generator point (g) in E_P (a, b). n_i is the value of a private key, where $n_i < n$ [smallest positive integer number is represented by n, where n * g = ⊗. Afterwards, the electrical node makes the generator point with the elliptic curve E_p (a,b) as publicly available. Then the electrical device, i calculates its public key as follows and communicates the data with SM:

$$P_i = n_i \times g \quad (6)$$

To perform encryption of data for connected SM (j), i calculates the coded pair of text with the help of a random number, k, as follows:

$$C_M = (kg, P_M + kP_j) \quad (7)$$

Here, P_M denotes the point of encoding for message M. Afterward, the message sensor node j runs the following decryption equation:

$$P_M + kP_j - n_j(kg) = P_M + k(n_j g) - n_j(kg) = P_M \quad (8)$$

Firstly, the node j identifies the starting or first point of cipher text and multiplies it with own private key, and then subtract this from the second point. Any malicious node that intends to connect to connect to the network must have the value of random number k to decode the message, and it is quite difficult to find the value of kg. The SM along with any other connected devices will exchange identification information among themselves for verification purpose, using the ECC. Confidential data will only be communicated once the authentication is completed using Salsa20 method that requires minimal electricity and processing power.

3.2.2 Data Exchange Stage

In the data exchange phase, the Salsa20 encryption methodology has been proposed in this paper due to its lightweight nature in terms of resource and power consumption. Salsa20 is a modified version of ChaCha20, and the length of input and output are both of 16 words [22]. Salsa20 algorithm uses a round function to operate continuously on same set of data to derive result, which is same as many other cipher algorithms. 4 nos quarter round functions make into the Salsa20's round function. The quarter round functions are as follows:

$$b^{\wedge} = (a + d) <<< 7; \quad (9)$$
$$c^{\wedge} = (b + a) <<< 9; \quad (10)$$

$$d^{\wedge} = (c + b) <<< 13; \quad (11)$$
$$a^{\wedge} = (d + c) <<< 18 \quad (12)$$

Here, a, b, c, d = words of initial state, with length 32 bits for each. The initial state matrix is comprised of 16 words; however, the quarter round function takes four number of words at a time to calculate, each of which is 32-bit in length.

4. RESULTS & DISCUSSION

4.1 Performance Analysis of ChaCha20-based encryption for Advanced Metering Infrastructures

Performance of the proposed scheme has been examined and analyzed mathematically in terms of computational energy requirement, processing time and throughput. To perform the analysis, Intel Core 2 Due CPU with 2.13 GHz processor has been used with voltage range of 0.8500V - 1.5V.

Computational Energy: To evaluate the energy requirement or computational energy of the recommended method and AES, the following equation has been used:

$$E = \frac{CC/B}{CC/S} IV \quad (13)$$

Here, CC/B = clock cycle per bytes, and CC/S = processor clock cycle, I = required power consumption in the entire process, and V = operating voltage of the processor. Comparison of computational energy for AES and ChaCha20 are presented in Figure 2 below.

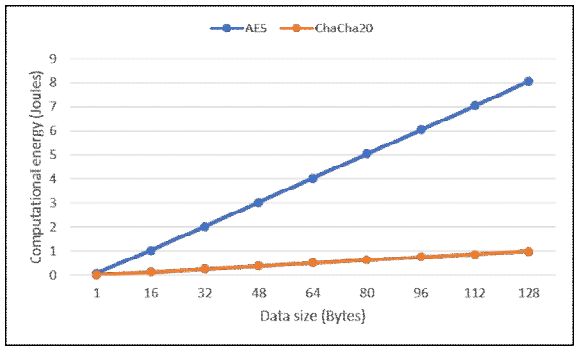

Figure 2: Comparison of Energy Consumption between AES and ChaCha20

It can easily be seen that ChaCha20 can process 128 bytes of data with 8 times lower energy compared to AES (8 Joules by AES compared to 1 Joule by ChaCha20).

Processing time: Less processing time for the operation indicates quicker and more efficient encryption method.
In this simulation, the required time can be calculated as,

$$t = \frac{DataSize}{Speed} \quad (14)$$

$$\text{Speed} = \frac{CC/S}{CC/B} \quad (15)$$

Here, speed = bytes per second. It can be seen clearly from Figure 3 that ChaCha20 processing time is significantly faster than AES.

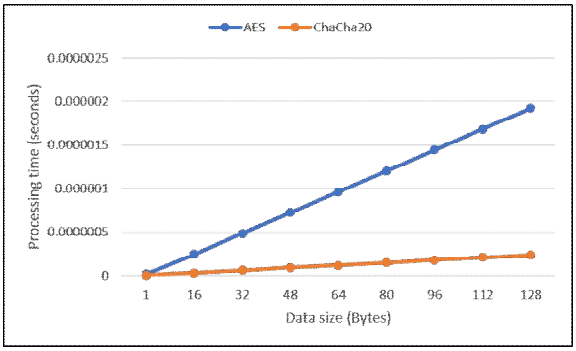

Figure 3: Comparison of Processing Time between AES & Chacha20

Throughput: Higher value of Throughput or amount of data processing per unit of time, generally indicates better performance for the system [27] [26]. The following equation has been used:

$$\text{Throughput} = \frac{Size\ of\ Data}{Encryption\ Time} \quad (16)$$

Figure 4 illustrates that the throughput of ChaCha20 is much better compared to AES.

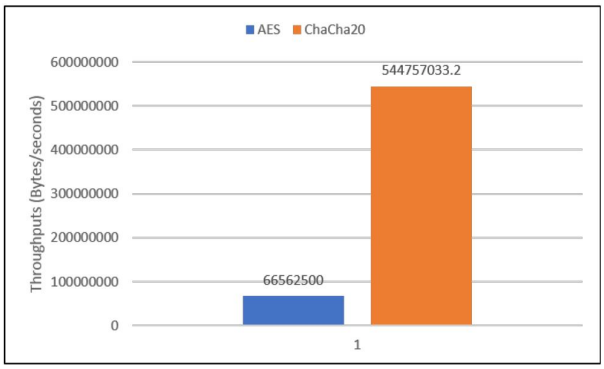

Figure 4: Throughput Comparison of AES and ChaCha20

4.2 Performance Analysis of Salsa20-based encryption for Smart Meter Communication

The performance of the prescribed encryption tool has been evaluated quantitively in terms of processing time and power consumption. For the analysis, an Intel Core 2 Duo CPU with 2.13 GHz of processing power has been used which operates with a voltage range of 0.85V to 1.5V.

The formula to calculate processing time and power consumption has been derived from [28]. Figure 5 illustrates the comparison of power consumption between ChaCha20 and Salsa20 methods, and accordingly, Salsa20 requires less amount of power to process the same amount of data as ChaCha20. For using in a small device such as SM, this characteristic of minimal power consumption for Salsa20 methods, is highly appropriate.

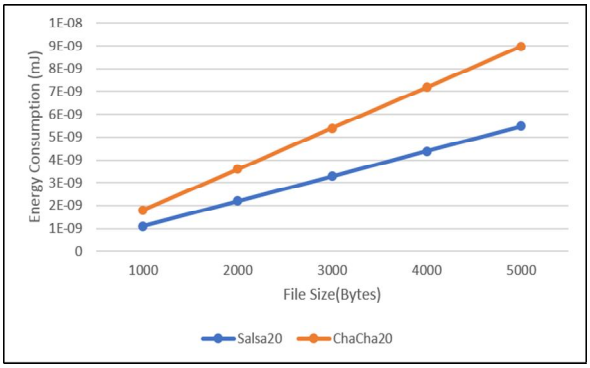

Figure 5: ChaCha20 and Salsa20: Comparison of Energy Consumption

Numerical representation of the processing time requirement comparison by both ChaCha20 and Salsa20 is shown in Figure 6. It shows that processing time for Salsa20 for similar data is less compared to ChaCha20 and in consequence, the devices that use Salsa20 will be able to communicate faster within the network.

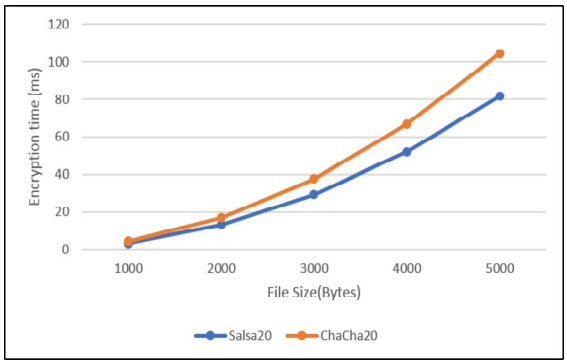

Figure 6: ChaCha20 and Salsa20: Comparison

5. CONCLUSION

With an objective to develop an efficient and effective encryption tool for smart grid and smart meter communications, this paper has evaluated the simulated performance of ChaCha20 and Salsa20 encryption tools. It has been taken into consideration that, the devices connected throughout the SG network are very limited in the processing power and require very fast communication within the system to realize the full potential of a smart grid through automation. For this purpose, ChaCha20 encryption has been proposed in this paper to use as a tool to encrypt and decrypt data within a SG network. A public and private key based verification method has been proposed to increase trustworthiness. Also, chaos based random number generation system has been applied to strengthen the system. Mathematical analysis of the simulation result shows that this method is appropriate to be used in SG network given the energy and resource limitations in mind, where it also protects the network from timing attacks. Apart from that, to protect SM communication, an ARX-based encryption technique known as Salsa20 has been proposed in this paper, which is a more lightweight and modified version of ChaCha20. On top of Salsa20, it is also prescribed that ECC-based data verification can be exercised before any data exchange without creating a huge demand for processing power and time within the system. ECC is based on public key and highly energy efficient. Quantitative analysis of both ChaCha20 and Salsa20 in terms of processing time and energy consumption suggests that Salsa20 is more energy-efficient encryption tool, which is also faster, making it a perfect choice for SM devices.

ACKNOWLEDGEMENT

This research has been made possible by the funding from the Ministry of Education Malaysia grant number LRGS/2018/UNITEN-UKM/EWS/04.

REFERENCES

1. El Pro Cus, **Types of Energy Meters and Their Working Principles**, [Online]. Available: https://www.elprocus.com/watt-hour-meter-circuit-working-with-microcontroller/. [Accessed 25 September 2019].
2. Electrical Study Notes, **Single Phase Energy Meter,** 28 March 2017. [Online]. Available: https://www.electricalstudynotes.com/2017/03/single-phase-energy-meter.html. [Accessed 22 September 2019].
3. A. Siddiqua, S. Begum, M. Y. A. Baig and C. Atheeq, **A Review and Techniques in Smart Grid for Authentication of Messages**, *International Journal of Latest Engineering and Management Research (IJLEMR)*, vol. 3, no. 3, pp. 91-96, 2018.
4. N. Komninos, E. Philippou and A. Pitsillides, **Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures,** *IEEE Communications Surveys & Tutorials*, vol. 3, no. 3, pp. 1933-1954, 2014. https://doi.org/10.1109/COMST.2014.2320093
5. X. Fan and G. Gong, **Security challenges in smart-grid metering and control systems,** *Technology Innovation Management Review*, Vol. 3, no. 7, 2013.

6. E. Bou-Harb, C. Fachkha, M. Pourzandi, C. Debbabi and C. Assi, **Communication security for smart grid distribution networks,** *IEEE Communications Magazine*, Vol. 51, no. 1, p. 42–49, 2013.
7. L. Wu, J. Wang, S. Zeadally and D. He, **Anonymous and efficient message authentication scheme for smart grid,** *Security and Communication Networks*, vol. 2019, 2019.
8. D. A. Chekired, L. Khoukhi and H. T. Mouftah, **Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid,** in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, 2019.
9. M. A. Mustafa, S. Cleemput, A. Aly and A. Abidin, **A secure and privacy-preserving protocol for smart metering operational data collection,** *IEEE Transactions ON Smart Grid*, 2018.
10. F. Skopik, Z. Ma, T. Bleier and H. Grüneis, **A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures,** *International Journal of Smart Grid and Clean Energy*, Vol. 1, no. 1, pp. 22-28, 2012. https://doi.org/10.12720/sgce.1.1.22-28
11. H. Kim, **Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks,** *International Journal of Distributed Sensor Networks* , 2012.
12. T. Bradley, **Stuxnet Compromise at Iranian Nuclear Plant May Be By Design,** PCWorld, 27 September 2010. [Online]. Available: https://www.pcworld.com/article/206320/stuxnet_compromise_at_iranian_nuclear_plant_may_be_by_design.html. [Accessed 12 September 2019].
13. T. Bradley, **SCADA Systems: Achilles Heel of Critical Infrastructure,** 27 September 2011. [Online]. Available: https://www.pcworld.com/article/230675/scada_systems_achilles_heel_of_critical_infrastructure.html. [Accessed 9 September 2019].
14. D. A. Chekired, L. Khoukhi and H. T. Mouftah, **Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid,** in *IEEE International Conference on Communications (ICC)*, 2019.
15. A. Hern, **Smart electricity meters can be dangerously insecure, warns expert,** The Guardian, 29 December 2016. [Online]. Available: https://www.theguardian.com/technology/2016/dec/29/smart-electricity-meters-dangerously-insecure-hackers. [Accessed 12 September 2019].
16. S. Garg, K. Kaur, G. Kaddoum, F. Gagnon, S. H. Ahmed and N. K. D. Jayakody, **LiSA: A Lightweight and Secure Authentication Mechanism for Smart Metering Infrastructure,** Cornell University, 2019.
17. Z. Kasiran, S. Abdullah and N. M. Nor, **An advance encryption standard cryptosystem in iot transaction,** *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 17, no. 3, pp. 1548-1554, March 2020.
18. M. M. Subashini, S. Das, S. Heble, U. Raj and R. Karthik, **Internet of Things based Wireless Plant Sensor for Smart Farming,** *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 1, no. 2, pp. 456-468, May 2018. https://doi.org/10.11591/ijeecs.v10.i2.pp456-468
19. Q. Wu and M. Li, **A Lightweight Authentication Protocol for Smart Grid,** *IOP Conference Series: Earth and Environmental Science*, Vol. 234, no. 1, 2019.
20. P. Gope and B. Sikdar, **Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication,** *IEEE Transactions on Smart Grid*, Vol. 10, no. 4, pp. 3953-3962, 6 June 2018.
21. D. Ghosh, C. Li and C. Yang, **A Lightweight Authentication Protocol in SmartGrid,** *International Journal of Network Security*, Vol. 20, no. 3, pp. 414-422, 2018.
22. D. J. Bernstein, **ChaCha, a variant of Salsa20,** *Workshop Record of SASC*, Vol. 8, pp. 3-5, 2008.
23. M. Hamdi, R. Rhouma and S. Belghith, **A very efficient pseudo-random number generator based on chaotic maps and s-box tables,** *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, Vol. 9, no. 2, pp. 481-485, 2015.
24. H. M. Al-Mashhadi, H. B. Abdul wahab and R. Hassan, **Chaotic Encryption Scheme for Wireless Sensor Network's Message,** in *World Symposium On Computer Networks and Information Security*, Tunisia, 2014.
25. W. Wang and Z. Lu, **Cyber security in the Smart Grid: Survey and challenges,** *Computer Networks*, Vol. 57, no. 5, p. 1344–1371, 2013.
26. N. Kumar and P. Chaudhary, **Performance evaluation of encryption/decryption mechanisms to enhance data security,** *Indian Journal of Science and Technology*, Vol. 9, no. 20, pp. 1-10, 2016.
27. D. Salama, H. A. Kader and M. Hadhoud, **Studying the Effects of Most Common Encryption Algorithms,** *International Arab Journal of e-Technology*, Vol. 2, no. 1, pp. 1-10, 2011.
28. A. Ahmad, A. Swidan and R. Saifan, **Comparative Analysis of Different Encryption Techniques in Mobile Ad Hoc Networks (MANETS),** *International Journal of Computer Networks & Communications (IJCNC)*, Vol. 8, no. 2, pp. 89-101, 2016. https://doi.org/10.5121/ijcnc.2016.8208