2023 International Conference on Digital Applications, Transformation & Economy (ICDATE) | 979-8-3503-1068-9/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICDATE58146.2023.10248469

Smart Energy Meter Implementation: Security Challenges and Opportunities

J. Remang ak Jambi
Department of Electrical and Computer Engineering
Curtin University Malaysia
Miri, Malaysia
johannesremang97@gmail.com

W. K. Wong
Department of Electrical and Computer Engineering
Curtin University Malaysia
Miri, Malaysia
weikitt.w@curtin.edu.my

Filbert H. Juwono
Department of Electrical and Electronic Engineering
Xi'an Jiaotong - Liverpool University
Suzhou, China
Filbert.Juwono@xjtlu.edu.cn

Foad Motalebi
Department of Electrical and Computer Engineering
Curtin University Malaysia
Miri, Malaysia
foad.m@curtin.edu.my

***Abstract*—The digital age has accelerated the development of smart energy monitoring technology (smart meter) that is crucial in our ever complex grid system. Smart energy meters are crucial element of the development of intelligent networking, measuring energy flow and communicating information on energy use between users and service providers, as well as monitoring and managing home appliances and gadgets using consumer data. They monitor consumption and generation of power in real time enabling consumer to be prosumer in energy. However, there are a number of obstacles that this technology may face. In this paper, the architecture, security concerns, and potential solutions to smart energy meter security are presented. In particular, a concise review of Internet of Things (IoT) security vulnerabilities that might possibly cause harm to the community is given, as well as some opportunities in this area. In addition, we explore the challenges and propose several options for researchers to make a more significant contribution. This research area can be considered as a sunrise development in most regions of the world and will continue to be a major development domain. In the future, researchers should see this research area as ”greenfield” features of research from a variety of perspectives, including hackability, criminology, and implementation standards.**

***Index Terms*—Smart energy meter, IoT, security**

TABLE I
COMPARISON OF TRADITIONAL ENERGY MONITORS AND SMART ENERGY MONITORS

Features	Normal Energy Meter	Smart Energy Meter
Basic Function	Measures total energy consumed	Measures total energy consumed
Data Display	Analog display	Digital display with real-time information
Reading Method	Manual Reading	Automatically sends readings to utility
Communication	No communication capability	Uses communication technologies (e.g. IoT)
Data Logging	No data logging functionality	Stores energy consumption data
Real-Time information	N/A	Provides real-time energy usage data
Billing	Based on periodic readings	Enables dynamic and accurate billing
Load Monitoring	N/A	Monitors and analyzes load patterns
Energy Consumption Analysis	N/A	Provides detailed energy consumption data
Integration with Smart Home	N/A	Integrates with smart home systems
Theft Detection	N/A	Detects energy theft or tampering

I. INTRODUCTION

Energy, in particular electricity, is widely regarded as the driving force behind modern socio - economic growth. Technology advancements enticed us to employ electricity-driven elements in all facet of our lives, from commercial to household, to make our lives more comfortable. However, new issues have arisen, necessitating ongoing research into how to manage the power supply-demand balance more effectively, securely, and reliably, as well as assuring coordinated multi-way communications for better network and user asset monitoring and control. Primarily, due to the more complex nature of consumer that also become a producer (prosumer), more complex nature of energy supply and consumption tracking have now become a necessity. The Internet of Things (IoT) is now a fast evolving field of technology that offers a wide range of cutting-edge capabilities across a copious of application domain [1]. By changing traditional energy monitors into modernized smart energy monitoring systems, IoT can address these inescapable challenges [2]. Table I show a comparison of traditional energy monitors and smart energy monitors.

The traditional energy monitoring system can be considerably improved by using an IoT-Based smart energy monitoring system with sophisticated two-way data transmission. These enhancements improve the system's dependability, adaptability, and efficiency. The conventional smart energy meter is a software-based, energy-efficient device that properly monitors

979-8-3503-1068-9/23/$31.00 ©2023 IEEE

and calculates energy usage. Meter readings can be sent wirelessly to distributors or users, obviating the requirement for a human meter reader. Both users and energy providers benefit from smart energy meters in terms of performance, reliability, and cost savings [3].

Although the IoT has enabled a far better and more efficient energy monitoring system, IoT implementation has its own set of obstacles. Within the IoT framework, for example, cyber-adversaries can launch cyber-attacks that cause serious damage such as compromising user data, altering user data, manipulating energy data analysis, and even causing physical damage to the user's end device. Potential technologies such as the blockchain technology [4], [5], machine learning and artificial intelligence [6], [7] can be utilized to address these issues as well as improve the efficiency of the smart energy monitoring system. This paper aims to discuss several aspects of the smart energy monitoring system.

II. Literature Review

A. Architecture of IoT Smart Energy Meter

In this section, we will cover the IoT smart energy monitoring system architecture, which is made of several state-of-the-art advanced technologies. Typically, the architecture is layer-based and various levels have distinct needs [8]. In this study, a three-layered architecture is used because it is suitable for smart energy meter integration. Such a three-layered structure is more applicable from the perspective of energy monitoring system requirements [8]. The three layers of the smart energy meter architecture are data collection layer, data communication layer, and data processing layer.

The data collection layer is in charge of gathering and sensing records and data. The data communication layer is in charge of transporting the data gathered in the data collection layer. It is the most important aspect of this design because it combines multiple communication infrastructure. Lastly, the data processing layer processes and displays data to the end user. It also keeps track of real-time data for forecasting and other purposes. For each layer of this architecture, a variety of cutting-edge technologies are available. The following sections discuss some essential enabling technologies.

Data Collection Layer Data collection layer is responsible for gathering data from physical devices using advanced sensing and actuation technologies, such as sensors [8]. A sensor is a device that detects or measures a change in a physical condition or event, such as temperature, light, noise, pressure, motion, and so on, and afterwards, indicates or reacts by generating an electronic signal [9]. The premise behind 'smart' energy monitoring is that it will operate on real-time data, and in order to do so, sensors must supply the real-time data. The data sensing operation in smart energy monitoring entails sensing and detecting many elements, such as voltage and current readings.

Data Communication Layer: A smart energy meter's data communication layer is a series of components combined with a micro controller unit (MCU) that communicates using various communication technologies. End-devices and gateways are the two categories of devices that are supported by this operating system [10]. End devices with MCUs are highly energy efficient and can support short-range low-power communication protocols. MCUs have become extremely complex and powerful in recent years with embedded communication modules, allowing for greater features and security for end devices. Due to the fact that end devices are resource-constrained, collection and transmission of data should occur in real time, with no buffering. This form of operating system is known as real-time operating system (RTOS), and it allows devices to be more productive [10].

Gateway devices are in charge of connecting a large number of IoT-enabled end devices to the cloud for data transmission, they must run on a more powerful, secure, and vigorous operating system which can support multiple communication protocols while also protecting the network from external attacks [10].

Data Processing Layer: This layer consists of a number of IoT system functional modules that handle data for smart energy meters. The layer processes the data and acts as the main platform for users to provide relevant analysis for decision-making processes. Artificial intelligence can be used for advanced data analysis in this layer, notably predictive analysis, machine learning, and computer vision [8]. Two commonly used tools that contribute to various fields for the processing and analysis of information or data are described below.

Cloud Computing: Cloud computing refers to the on-demand access of computer system such as servers, storage and networking, allowing companies to create and operate their own programs, data, and operation systems. Cloud computing is critical for providing universal, adequate, on-demand network access to servers, storage, applications, etc. which can be automatically made available and released with minimal effort from service providers. The term ”cloud” refers to data centers that are scattered across several geographical areas and made available to a large number of users over the internet. Cloud computing allows huge data storage as well as extremely dependable, flexible, and autonomous processing [10]. This cloud is used in the IoT smart energy meters to aggregate all data and information collected from various elements such as sensors, appliances, as well as other devices, then process, analyze, and provide the results to end users (consumers or service providers) for additional insight.

Fog and Edge Computing: Fog computing and edge computing are distributed computing approach that moves data processing and storage nearer to the end device. They improve response time and bandwidth utilization while also allowing for decision-making. Smart energy meter data can be used for a variety of purposes, including revenue side monitoring and energy savings through power demand identification and irregularity detection [11]. Furthermore, a great number of devices, such as smart energy meter IoT devices, are generally used to provide a convenient atmosphere for users to generate a significant amount of information that must be processed locally in order to minimize network traffic [12]. Edge computing improves the localized computation system by allowing edge devices to make decisions based on locally processed data. The edge device can act accordingly without waiting for cloud analysis. Edge computing decentralizes the system and reduces the risk of single-point failure by bringing data analysis and decision-making to the network's edge [10].

The number of IoT-enabled entities raises network traffic since they need to transfer data to the cloud for any further processing, which necessitates greater capacity. As a result, it becomes a limitation for cloud-based systems, as there has been less advancement (such as enhancing CPU processing power) to increase data transmission bandwidth in comparison with other technologies [10]. Edge computing and Fog computing solve this problem by calculating and storing data nearer to the data source, then sending the reduced data into the cloud via the internet. Fog computing minimizes the volume of data transferred to the cloud while also improving system reaction time and lowering network latency. It also has the benefit of preventing a single point of failure. If the connectivity is lost, the edge device will continue to collect and process data locally from end devices before sending it to the cloud once the connection is restored.

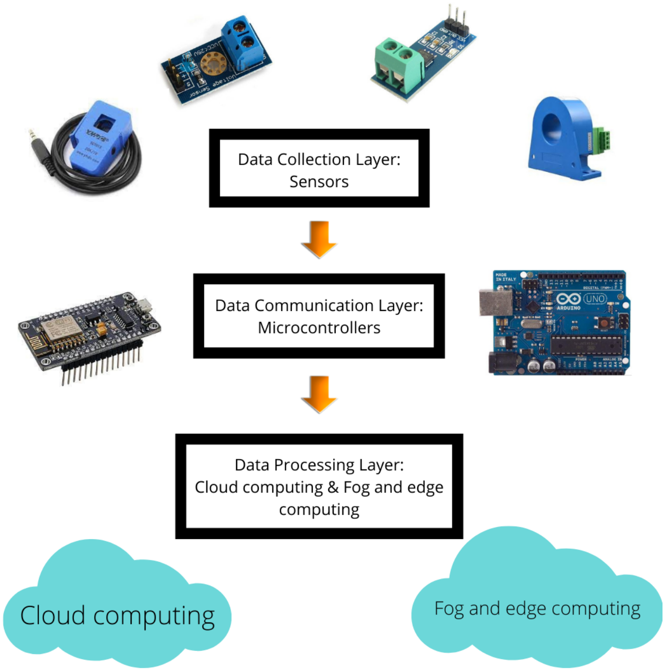

Fig. 1. Layers of smart energy meter architecture

III. Security Concerns

Although IoT Based smart energy meter is a very convenient device to use, it has its own disadvantages when it comes to security. IoT based smart energy meters, like any other equipment linked to a network, are subject to attacks aimed at stealing data or manipulating readings. Adversaries avail from attacking smart energy meters as they can utilize these frailties to compromise or steal user's data to appease their needs. For example, a tech-savvy criminal can inspect a homeowner's absence from their home by checking their power consumption. Another example is that adversaries can use the data obtained from the attacks to carry out extortion against the victims. The following section will discuss the type of attacks that can occur in a smart energy meter environment.

Spoofing and Altering routing: Spoofing and altering routing primarily target routing information where data between nodes are exchanged. Spoofing attacks are carried out by sending a fake error message, causing a routing loop, and a variety of other methods [13]. Spoofers do not emit a signal at first, instead listening to the proper transmitter. When the legal transmitter ceases transmitting a signal to its receiver, the spoofer begins transmitting the faulty signal [14]. For example, in the IoT application login of smart energy meter, a pop up ad mirror the login tab, and when pressed, it will redirect the user to a fake IoT application login page. The user will try to login through that fake login page. There the user's credentials will be recorded by the fake login page.

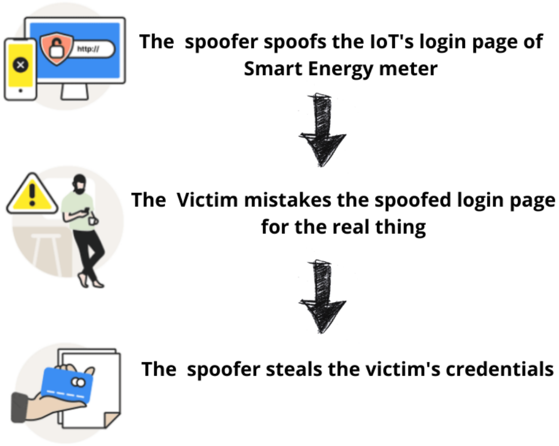
The spoofer spoofs the IoT's login page of Smart Energy meter
The Victim mistakes the spoofed login page for the real thing
The spoofer steals the victim's credentials
http://

Fig. 2. Spoofing attack through smart energy meter's IoT login page

Sybil Attacks: A Sybil attack is defined as a single node that represents itself as a multiple identities [13]. Sybil attacks are a major danger to the integrity of any device that uses a Wireless Sensor Network (WSN), such as a smart energy meter network. A singular malicious node forges numerous entities inside a network to deceive the legitimate nodes in this type of attack. By inventing new identities or stealing legitimate identities, the malicious node displays many identities to other nodes [15] [16] [17]. This jeopardizes the user's security and privacy. An attacker merely needs to gain control of network nodes, obtain data from these nodes, and construct false nodes to initiate their identities. After gaining network control, the attacker can impose prohibition, preventing the user from properly utilising the smart energy meter's network.

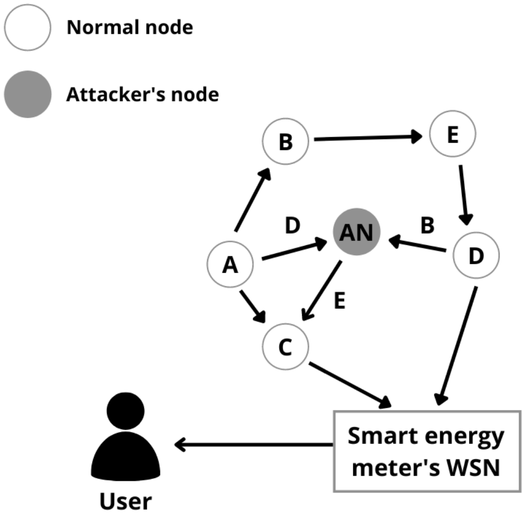

Fig. 3. Sybil attack on a smart energy meter's network. 'AN' appears to be node 'D' for node 'A', node 'B' for node 'D' and node 'E' for node 'C' so when it comes to node 'C' wanting to communicate with node 'E' it actually communicate with node 'AN'

Denial of Service (DoS): By conducting a DoS attack, an attacker attempts to disrupt or shut down the network. A DoS attack is an attack on either a network or computational resource that can result in reduced network capacity [18], [19]. A DoS attack is one in which a computer floods a server using Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) packets. In [20], for example, the researchers use a constructed smart meter using a Smartpi device, a Raspberry featuring a module that allows it to function as a smart meter and detect voltages, currents, and powers, to simulate a DoS attack. The DoS attack is conducted with a varying number of attackers, with the reaction time and fraction of dropped packets owing to congestion, as well as the state of the target device's CPU, being monitored. This exploit is undetectable by software and leaves no trace. However, a DoS attack is a possibility because the systems function normally on their own, but faults occur once they communicate with one another. The concept of this particular type of attack is shown in Fig. 4.

Man-in-the-Middle Attacks (MITM): In MMITM attack, the attacker gains entry to the communication channel between two endpoints and manipulates the messages. As a result, a malicious third-party attacker can collect, edit, replace, or manipulate data sent through the communication channel among the two endpoints. For example, an attacker can read the contents of a user's smart energy meter and decide to alter the data in a user's smart meter. The illustration of this attack is shown in Fig. 5.

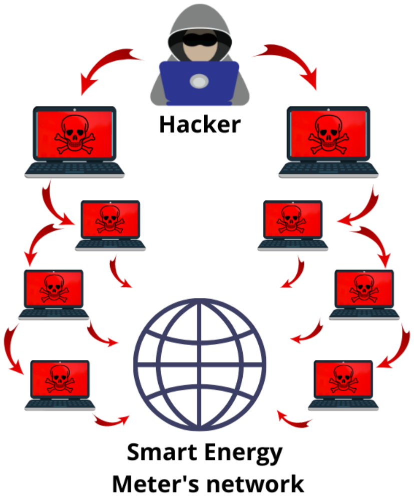

Fig. 4. An example of DoS attack, an attacker uses a network of hijacked computers to flood a smart energy meter's network with fraudulent request.

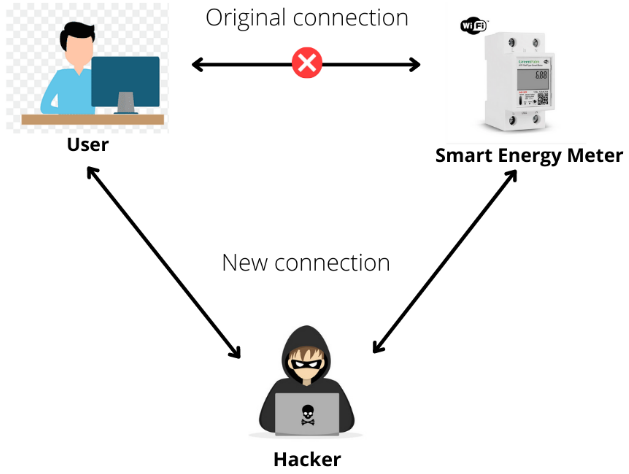

Fig. 5. Man-in-the-middle attacks on a smart energy meter.

Malware Attacks: Malware attacks are widespread cyber attacks that execute malicious apps on a victim's system, threatening essential security and privacy [21]. In the instance of smart energy meters, the attacker can utilize a malware attack to compromise the device's integrity. The use of malware that alters the way devices are designed and sets the values of readings (which are saved in a database) to zero during a certain time period compromises integrity [20], [22]–[24]. If the readings are shared with an unauthorized third party, the smart energy meter's confidentiality will be compromised.

TABLE II
ATTACKS ON IOT-BASED DEVICE .

Type of Attacks	Authors
Spoofing attack	[26], [27], [28], [29]
Sybil attack	[30], [31], [32], [33], [34]
Denial of Service (DoS) attack	[35], [36], [37], [38], [39]
Man-in-the-Middle attack	[39], [40], [41], [42]
Malware attack	[43], [44], [45], [46]

This resembles a scheme to deceive the power company by pretending to use less electricity. In servers or full scale computers, processing power is higher, thereby various more computation intensive approach can be deployed to detect malware such as using imaging ([25]) or analyzing dump memory. However, internal processors in smart meters are normally RTOS based processors which makes detection a niche challenge. An example is shown in [20] where an overview of how a malware attack is used. The researcher exploits the flaws in a Node-RED programming tool to construct phoney data flows that enter the database and change the power readings to a secondary value. the visualisation of this type of attacks is shown in 6. The summary of various types of attacks is shown in Table II.

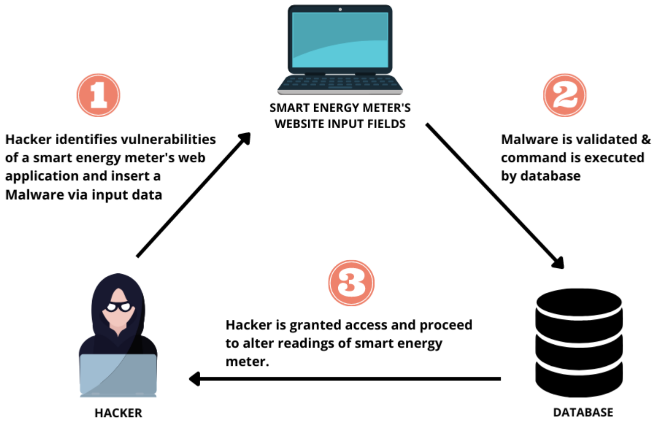
1
Hacker identifies vulnerabilities of a smart energy meter's web application and insert a Malware via input data
SMART ENERGY METER'S WEBSITE INPUT FIELDS
2
Malware is validated & command is executed by database
3
Hacker is granted access and proceed to alter readings of smart energy meter.
HACKER
DATABASE

Fig. 6. An example of a Malware attack in a smart energy meter.

IV. Further Opportunities to Enhance Adoption of Smart Meter System

A. Continuous Role of ”White Hat” Approach in Security

With the various security challenges, there certainly exist plenty of opportunities in improving the security of the IoT devices. Almost in every aspect, the smart meter is an IoT device similar with IP cameras or servers. However, these devices can be regulated by the utility companies to further enhance security of the devices. As discussed in the previous section, various cyber attack modes may arise in a planned attack such as Sybil or DoS attacks. With various scams that are currently ongoing, these attacks can be plan in tandem with the various physical or social scams. For example, the malignant parties may consider bringing down smart meters and subsequently offer their service in the pretense of ”mitigating” the issues. As such, there exist various scam strategies that have yet to be detected. One tested approach is by using preemptive measures to investigate the various possible cyber attack schemes and hybrid schemes. Smart meters may also incorporate Physically Unclonable Device as part of the enhancement scheme. This concept makes use of physical identifier in the semiconductor that enhances security to devices as identifier are physically embedded in the device rendering it virtually unclonable. From the aspect of cyber security, criminology, there exist various mitigation strategies that are yet to be explored. A white hat approach can be deployed to discover new scam or security loopholes as pre emptive approach. This presents a ”blue ocean” approach as the research domain may increase with discoveries of new possible schemes.

B. Emphasizing Benefits in Digitization

The integration of smart grid in certain parts of the world is still in its infancy. This cost and Return of Investment (ROI) factors weighs in heavily on the mass adoption of smart meter system. There is no clear benefit in implementing due to unjustified investment. In ASEAN countries, most of the countries are still adopting manual meter reading approach in general. However, smart meters with online capabilities are starting to gain traction especially in prosumers that have investments in residential solar panels. In such cases, production is constantly monitored for maintenance issues.

Utilities companies in different regions will need to consider these issues when considering adopting smart meter technology. For example, from the perspective of countries that do not adopt smart grid system of enabling the consumer to be prosumer, it is difficult to justify usage of smart meter system. In Malaysia, large scale roll out targeting 9.1 million users by 2026 is carried out by the electricity company TNB. Fig. 7 displays three types of smart meter utilising radio frequency, powerline communication system, and cellular communication system. Most of the current role is to implement radio communication utilizing pole mounted radio transceivers. As such, the cost would include the communication infrastructure as well as the smart meter units. Would this cost be absorbed by the user? How would the respond from user be perceived? It has been reported that there are many health rumours reported on the meter installation. How would the these rumours be countered with the right channel of information? In any case, solving problems with smarter meters and better analytics may encourage large scale adoption. In Malaysia, despite the mass adoption of solar panel in residential areas, selling the harvested energy to neighbours is still not permitted. As such, prosumers may only sell to the utilities companies. One of the challenges in utilities companies is curbing electricity theft. This apparent benefit may be highlighted as a strong justification in this specific application. Rapid stealing and illegal wiring of electricity can be identified with more advance meter features. The usage of smart meter will enable more data to curb such cases and to be able to monitor theft more efficiently. These issues surrounding digitization opportunities may provide researchers with more research questions for exploration.

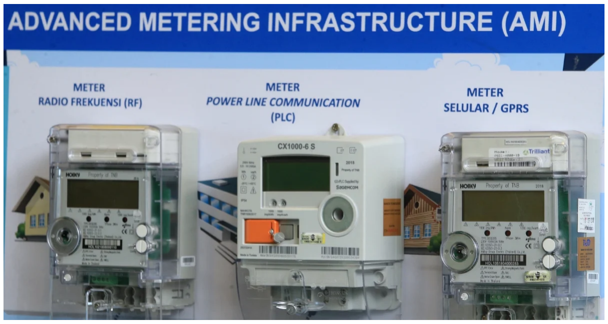

Fig. 7. Smart meter roleout by Malaysian Utilities provider TNB.

C. Legal Frameworks and Standards

One of the biggest challenges with regards to wider adoption in smart meters is with respect to legal and standards that are currently unavailable. This pertains to the slow or non-existing standards due to the lack of usage of the system. Most of the countries adhere to IEC standards, However, the standards at the moment cover mostly on analog and digital meters with regards to installation. It is noted that in some parts of the world standards developed by ANSI are used, sometimes as alternatives to IEC standards (Smart Energy International 2/2003). Until such standards are adequately available, there is a need to investigate and contribute to such standards especially with regards to security issues. This will constitute an important contribution from researchers in this domain. Many countries, particularly those in ASEAN, lack proper cyber laws, much alone in systems relevant to smart meter systems. For example in Malaysia, laws pertaining to cyber security (Computer Crimes Act 1997) may not be sufficient to persecute crimes that are specific to IoT and in more specifically (smart metering related crimes).

V. Conclusion

In this paper, various issues pertaining to implementation of smart meter have been discussed. The benefits and possibilities of such implementation are apparent to both consumers and stake holders. In addition, the architectures of smart energy meters, namely the data collection layer, data communication layer, and data processing layer have been discussed. Some of the network security concerns consisting of numerous attacks, i.e., spoofing and altering routing attacks, Sybil attacks, DoS attacks, MITM attacks, and Malware attacks, have been highlighted. How these malignant strategies can be used adversely for security from the view point of smart meter system has also been presented. Opportunities to enhance adoption of smart meter systems have been further discussed by highlighting the continuous role of ”white hat” approaches in ensuring security, emphasizing benefits in digitization and wider adoption legal frameworks and standards pertaining to the smart energy meter. These strategies have been highlighted in detail and case study presented. As the technology has just gained traction, many security challenges will arise as the cyber criminals explore further on the opportunities. Hence, this provides researchers sufficient room to explore on these challenges.

References

[1] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, “Secure healthcare data aggregation and transmission in iot—a survey,” *IEEE Access*, vol. 9, pp. 16 849–16 865, 2021.

[2] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons, F. Ponci, and A. Monti, “A cloud-based smart metering infrastructure for distribution grid services and automation,” *Sustainable Energy, Grids and Networks*, vol. 15, pp. 14–25, 2018.

[3] B. Heamath and C. V. P. Rao, “A study on smart meter and its significance,” in *International Journal of Research in Advanced Engineering and Technology*, vol. 2, no. 5, 2016, pp. 72–74.

[4] D. Minoli, “Positioning of blockchain mechanisms in iot-powered smart home systems: A gateway-based approach,” *Internet of Things*, vol. 10, p. 100147, 2020.

[5] M. U. Hassan, M. H. Rehmani, and J. Chen, “Privacy preservation in blockchain based iot systems: Integration issues, prospects, challenges, and future research directions,” *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[6] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, “Toward a lightweight intrusion detection system for the internet of things,” *IEEE Access*, vol. 7, pp. 42 450–42 471, 2019.

[7] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, “Applications of artificial intelligence and machine learning in smart cities,” *Computer Communications*, vol. 154, pp. 313–323, 2020.

[8] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, “Adopting internet of things for the development of smart buildings: A review of enabling technologies and applications,” *Automation in Construction*, vol. 101, pp. 111–126, 2019.

[9] S. E. Bibri, “The iot for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for environmental sustainability,” *Sustainable cities and society*, vol. 38, pp. 230–253, 2018.

[10] D. Mocrii, Y. Chen, and P. Musilek, “Iot-based smart homes: A review of system architecture, software, communications, privacy and security,” *Internet of Things*, vol. 1, pp. 81–98, 2018.

[11] T. Sirojan, S. Lu, B. T. Phung, and E. Ambikairajah, “Embedded edge computing for real-time smart meter data analytics,” in *2019 International Conference on Smart Energy Systems and Technologies (SEST)*, 2019, pp. 1–5.

[12] R. Kalra, N. Singh, and S. Gupta, “Fogmeter: Smart metering solution based on fog computing,” in *2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON)*, 2020, pp. 22–27.

[13] D. N. Sushma and V. Nandal, “Security threats in wireless sensor networks,” in *IJCSMS International Journal of Computer Science Management Studies*, vol. 11, no. 01, 2011, pp. 59–63.

[14] M. H. Yılmaz and H. Arslan, “A survey: Spoofing attacks in physical layer security,” in *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)*, 2015, pp. 812–817.

[15] J. R. Douceur, “The sybil attack,” in *International workshop on peer-to-peer systems*. Springer, 2002, pp. 251–260.

[16] Z. Su, C. Lin, F. Ren, and X. Zhan, “Security mechanisms analysis of wireless sensor networks specific routing attacks,” in *2006 First International Symposium on Pervasive Computing and Applications*. IEEE, 2006, pp. 579–584.

[17] D. G. Padmavathi, M. Shanmugapriya *et al.*, “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” *arXiv preprint arXiv:0909.0576*, 2009.

[18] E. Alsaadi and A. Tubaishat, “Internet of things: Features challenges and,” 2015.

[19] A. Belapurkar, A. Chakrabarti, H. Ponnapalli, N. Varadarajan, S. Padmanabhuni, and S. Sundarrajan, *Distributed systems security: issues, processes and solutions*. John Wiley & Sons, 2009.

[20] R. P. Díaz Redondo, A. Fernández-Vilas, and G. Fernández dos Reis, "Security aspects in smart meters: Analysis and prevention," *Sensors*, vol. 20, no. 14, p. 3977, 2020.

[21] M. R. Khouzani, S. Sarkar, and E. Altman, "A dynamic game solution to malware attack," in *2011 Proceedings IEEE INFOCOM*, 2011, pp. 2138–2146.

[22] Y. Guo, C.-W. Ten, S. Hu, and W. W. Weaver, "Preventive maintenance for advanced metering infrastructure against malware propagation," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1314–1328, 2015.

[23] P. Eder-Neuhauser, T. Zseby, J. Fabini, and G. Vormayr, "Cyber attack models for smart grid environments," *Sustainable Energy, Grids and Networks*, vol. 12, pp. 10–29, 2017.

[24] Y. Park, D. M. Nicol, H. Zhu, and C. W. Lee, "Prevention of malware propagation in ami," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2013, pp. 474–479.

[25] W. K. Wong, F. H. Juwono, and C. Apriono, "Vision-based malware detection: A transfer learning approach using optimal ecoc-svm configuration," *IEEE Access*, vol. 9, pp. 159 262–159 270, 2021.

[26] P. Kumar, A. Gurtov, M. Sain, A. Martin, and P. H. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4349–4359, 2019.

[27] B. Chatfield and R. J. Haddad, "Rssi-based spoofing detection in smart grid ieee 802.11 home area networks," in *2017 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2017, pp. 1–5.

[28] S. Raguvaran, "Spoofing attack: Preventing in wireless networks," in *2014 International Conference on Communication and Signal Processing*, 2014, pp. 117–121.

[29] N. Wang, S. Lv, T. Jiang, and G. Zhou, "A novel physical layer spoofing detection based on sparse signal processing," in *2015 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2015, pp. 582–585.

[30] A. Rajan, J. Jithish, and S. Sankaran, "Sybil attack in iot: Modelling and defenses," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017, pp. 2323–2327.

[31] R. Hadiansyah, V. Suryani, and A. A. Wardana, "Iot object security towards the sybil attack using the trustworthiness management," in *2020 8th International Conference on Information and Communication Technology (ICoICT)*, 2020, pp. 1–4.

[32] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[33] J.-D. Kim, M. Ko, and J.-M. Chung, "Novel analytical models for sybil attack detection in ipv6-based rpl wireless iot networks," in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, 2022, pp. 1–3.

[34] A. Tandon and P. Srivastava, "Trust-based enhanced secure routing against rank and sybil attacks in iot," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 2019, pp. 1–7.

[35] M. Daud, R. Rasiah, M. George, D. Asirvatham, A. F. A. Rahman, and A. A. Halim, "Denial of service: (dos) impact on sensors," in *2018 4th International Conference on Information Management (ICIM)*, 2018, pp. 270–274.

[36] L. Liang, K. Zheng, Q. Sheng, and X. Huang, "A denial of service attack method for an iot system," in *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, 2016, pp. 360–364.

[37] E. A. Asonye, I. Anwuna, and S. M. Musa, "Securing zigbee iot network against hulk distributed denial of service attack," in *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, 2020, pp. 156–162.

[38] Y. Cui, Q. Liu, K. Zheng, and X. Huang, "Evaluation of several denial of service attack methods for iot system," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*, 2018, pp. 794–798.

[39] G. R. Andreica, L. Bozga, D. Zinca, and V. Dobrota, "Denial of service and man-in-the-middle attacks against iot devices in a gps-based monitoring software for intelligent transportation systems," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, 2020, pp. 1–4.

[40] S. K, S. V, A. Singh, A. R, H. Saxena, and S. S. S, "Detection and mitigation of man-in-the-middle attack in iot through alternate routing," in *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, 2022, pp. 341–345.

[41] A. B. M. Sultan, S. Mehmood, and H. Zahid, "Man in the middle attack detection for mqtt based iot devices using different machine learning algorithms," in *2022 2nd International Conference on Artificial Intelligence (ICAI)*, 2022, pp. 118–121.

[42] O. Toutsop, P. Harvey, and K. Kornegay, "Monitoring and detection time optimization of man in the middle attacks using machine learning," in *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, 2020, pp. 1–7.

[43] T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari, and E. Magesh, "Mitigating mirai malware spreading in iot environment," in *2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2018, pp. 2226–2230.

[44] S. M. Pudukotai Dinakarrao, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad, and H. Homayoun, "Lightweight node-level malware detection and network-level malware confinement in iot networks," in *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*, 2019, pp. 776–781.

[45] V. Clincy and H. Shahriar, "Iot malware analysis," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, 2019, pp. 920–921.

[46] A. Mahboubi, S. Camtepe, and K. Ansari, "Stochastic modeling of iot botnet spread: A short survey on mobile malware spread modeling," *IEEE Access*, vol. 8, pp. 228 818–228 830, 2020.