SOUTHEAST ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Volume 8, Issue 1, 2023
P-ISSN: 2672-2984
E-ISSN: 2672-2992
www.sajst.org

Cybersecurity of Smart Grids: Attacks and Defenses of the Smart Meters in an Advanced Metering Infrastructure (AMI)

Gian Lloyd B. Jacoba[1] and Gerry Paul C. Genove[1]
[1]Saint Louis University, Baguio City, Benguet, Philippines

Article Info:
Received: ***25 Aug 2023;*** *Revised:* ***05 Dec 2023;*** *Accepted:* ***20 Dec 2023;*** *Available Online:* ***31 Dec 2023***

Abstract - With rising energy demand, newer challenges come with it. The paper analyzes the cybersecurity challenges and defenses accompanying the smart grid, particularly Smart Meters in an Advanced Metering Infrastructure (AMI). The Advanced Metering Infrastructure provides intelligent systems connecting the customers and the energy service providers. These AMIs are essential in keeping track of the customer's data because of their real-time capability and smart options that were integrated. It is then necessary to protect the AMI because it can cripple entire smart grids and leave the population vulnerable to elements. Based on the literature review, the most common attacks in the AMI are Eavesdropping, Denial of Service, False Data Injection, Remote Connect/Disconnect Firmware Manipulation, Man-in-the-Middle, and Power Hijacking. The most potent defenses the literature review has found to employ are Data Encryption, Authentication, and Intrusion Detection Systems.

Keywords: Cybersecurity of Smart Meters, Blockchain, Machine Learning, Cryptography

INTRODUCTION

With our population hitting 8 billion (Subramaniam, 2022) the rising demand for energy in our time resulted in a plethora of efforts to integrate intelligent systems into the electric grid to adapt to the rising needs of the consumers. The said intelligent integration to the grid not only allows the transformation of antiquated technologies to innovative communication techniques, but also transforms closed power control systems into open data networks (Ghelani, 2022).

A massive distributed computing platform such as the smart grid is created by integrating processors into each component of the power systems, each of which has a reliable operating system and autonomous agents connected to smart sensors linked to its own component or substation (Otuoze et. al., 2018). The processor enables access to its own operating conditions and reports its status to its neighboring components through communication lines, circuit breakers, and communication ports for the processors (Azad et. al., 2019). These advantages, which include regulated supply and demand, decreased downtime, fewer failures, lower grid losses, monitoring power consumption, demand side management (DSM), improved optimized network traffic, and generally better grid operations and services, are being provided by the modernization of conventional power systems all over the world (Mrabet et. al., 2018).

Back in 2010, the National Institute of Standards and Technology or the NIST proposed a framework wherein the future electrical grid is guaranteed with reliable, scalable, secure, interoperable, and manageable operation of the grids while being cost-effective (Gopstein et.al, 2021). NIST has defined the Smart Grid as “electricity with a brain”, which is technically a modernized grid which enables two-way communication of energy which leads to newer functionalities and applications.

It has seven logical domains, mainly, bulk generation, High Voltage Transmission and distribution, customers, markets, operations, and electricity service providers. The architectural model comprises many customer kinds that are categorized under various networks. These are industrial area networks (IANs), home area networks (HANs), and building area networks (BANs). Advanced metering infrastructure (AMI) is deployed for metering to track each inbound and outbound flow of electrical energy (Gopstein et.al, 2021). The smart grid has three components, mainly, the AMI, the SCADA or the Supervisory Control and Data Acquisition, and the third is communication standards and protocols. AMI is an integrated technology that creates intelligent relationships between customers and service providers. It is utilized for metering client energy on real-time energy pricing with cutting-edge capabilities to reduce energy usage (Gopstein et.al, 2021).

Comprising of three main components, the smart grid includes the AMI, the SCADA (Supervisory Control and Data Acquisition), and communication standards/protocols. The AMI serves as an integrated technology fostering intelligent relationships between customers and service providers. It facilitates real-time energy pricing and employs advanced features to optimize energy usage, contributing to a more efficient and responsive energy grid (Gopstein et al., 2021). Although smart grids give its consumers benefits to power their homes and businesses, with the integration of intelligent systems, it has opened up another set of challenges that we need to look out for, cyber-attacks (AVCI, 2021). Cyber security professionals need to be familiar with the grid and the value of security solutions that can meet the strict requirements of the grid for availability, efficiency, and scalability.

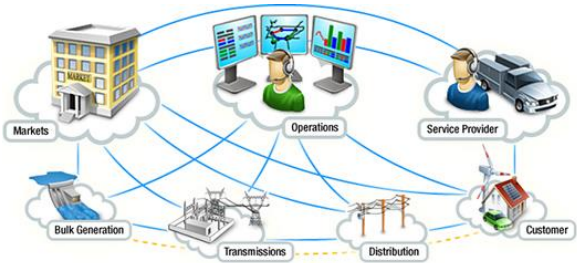

Fig. 1. NIST Smart Grid Framework 4.0 (Gopstein et.al, 2021)

Additionally, the grid's effects on cyber security must be understood by those who design and run it (Kawoosa & Prashar, 2021; Kimani, Oduol, & Langat, 2019). The demands of a smart grid communication system working safely in open data communication networks like the internet are unlikely to be met by legacy cyber security solutions created for commercial networks (Philips, Jayakumar, & Lydia, 2020). Smart grid communication networks are different from standard commercial network systems in terms of goals, objectives, and presumptions on what has to be guarded in terms of cyber security (Kawoosa & Prashar, 2021). To disrupt the smart grid system, attackers may exploit vulnerabilities. These threats may be terrorism, cyberattacks, vandalism, theft, etc. Natural catastrophes, known system disruptions, voltage and frequency instability problems, and inconsistent government policies and implementations are some additional potential hazards (Ul Haq et.al, 2017). As a result, any assault in one domain might potentially have an effect on the other domain and cause cascading failures, which include the Advanced Metering Infrastructure. (Blackouts, losses in finances, etc.).

The most critical component of Smart Grid is the Advanced Metering Infrastructure (AMI), which supports the system's effectiveness, sustainability, and dependability. Therefore, the potential for cyber-attacks in the AMI significantly influences Smart Grid's ability to operate reliably and effectively (Philips, Jayakumar, & Lydia, 2020). AMI makes the link between advanced meters and the smart grid possible through communications, the associated systems, and data management. AMI enables the gathering and delivery of information to consumers and other parties.

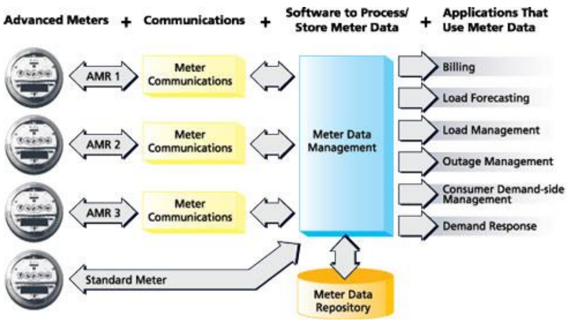

Fig. 2 Advanced Metering Infrastructure (Waters, 2006).

A successful Smart Grid attack might cause a blackout if there is a localized or widespread denial of the electricity service (Ghelani, 2022; Gopstein et. al, 2021). For instance, on February 24, 2022, during the initial hours of the military invasion of Russia, significant cyber warfare operations were launched against the Ukrainian energy utilities. Although the full impact of the operations has not yet been fully determined, it was revealed that the cyberattacks' stated goal was to destroy data from power plant utility control rooms, which resulted in widespread blackouts across Ukraine, including Kiev (Aljohani, 2022). Similar circumstances occurred in 2016 when hostile actors knocked out electricity to more than 200,000 Ukrainians. As a preventative measure to lessen AMI assaults, it is necessary to discover security flaws and attack mitigation techniques (Otuoze et. al., 2018). It is therefore important that as technology advances and the dangers associated with smart grids are more understood, this knowledge must also be updated.

One component of the AMI is the Smart Meter, and according to Fan and Gong (2013), a smart meter comprises several parts, including a microprocessor, a metering board, and a communication board. Interestingly, the metering board measures real-time power consumption under the microcontroller's control. The data is sent through the communication board to the substation and home area networks. Smart meters and household appliances can communicate with each other through Wi-Fi, ZigBee, Ethernet, HomePlug, Wireless M-Bus, and the like. A disconnect feature that, if enabled, enables utility providers or users to connect or disconnect household services and appliances remotely may also be present in the smart meter.

Accordingly, some of the features mentioned by Kawoosa and Prashar (2021) of smart meters are the following:

- Energy Prepayment.
- Anti-tampering and fraud detection.
- Remote and full customizable load limiter.
- Remote installation and update of firmware upgrades to accommodate new features.
- Real-time reaction to pricing signals received from the utility company.
- Real-time monitoring of power use, recording it, and transmitting the registers to the utility company or other energy provider services.
- Observing and updating the utility provider, the client and outside parties about the quality of power coming through.
- Monitoring consumer usage metrics, such as overall energy used, and maintaining a historical record.
- Remote connection and disconnection of customers from the grid.
- Notifying power companies in case power failures occur.

The smart meter is a crucial cyber security component that needs specific protection, as is evident from the description provided above, especially given that it also serves as the gateway to the overall Smart Grid system and, in certain situations, the Smart Home gateway. The utility center, the energy market, and consumers' residences are all connected through the Advanced Metering Infrastructure (AMI) network (AVCI, 2021; Kawoosa & Prashar, 2021). Therefore, since threats are always evolving, there is a need to constantly monitor and update the defenses that are being produced. This paper will then do a literature review of the attacks and the defenses that are being proposed because of the need stated beforehand.

Cybersecurity experts may find knowledge for potential solutions they may apply through this literature review. Additionally, it aids in the advancement of research into Smart Grids and the security of AMIs, which in turn aids in the development of privacy and cybersecurity solutions. Therefore, this paper studies the AMI from a networking security view to better understand the Cybersecurity concerns of the AMI and explore its difficulties and present solutions. The paper will review AMI to identify the problems and obstacles that impact its operation and suggest remedies. To do this, the following research questions will be addressed in this paper:

1) What cybersecurity problems and difficulties are now affecting the Smart Grid, especially in the AMIs (Smart Meters)?
2) What defenses and algorithms have been put up to address the cybersecurity problems and difficulties associated with AMIs (Smart Meters)?
3) Which of the above defenses would be suggested in addition to addressing the problems and difficulties related to the cybersecurity of AMIs (Smart Meters)?

The paper is organized as follows: Chapter 2 describes the methodology which is used in the paper, Chapter 3 will be discussing the results and literature gathered. Chapter 4 will be discussing the conclusion, and Chapter 5 introduces future work for the topic.

METHODOLOGY

A literature search was conducted using Google Scholar and EBSCO Host to address identified research questions. Google Scholar, chosen as the primary tool, retrieved scholarly and peer-reviewed literature from various databases such as arXiv, ERIC, MDPI, ResearchGate, among others. The search utilized keywords "cybersecurity of smart grids," "cybersecurity of advanced metering infrastructure," and "smart grids and AMI" to focus specifically on discussions related to the cybersecurity of AMI in smart grids.

Criteria

To further filter down the literature being brought up by EBSCOHost and Google Scholar, a criteria was followed based on Rothstein's guidelines. The following criteria was utilized:

1.) Published within the last 5 years.
2.) Written in English
3.) The paper should be peer-reviewed
4.) Published by a reputable Institution
5.) The contents of the paper are relevant to the topic.

Identification of Cybersecurity Issues revolving around the Smart Meters in AMI

The criteria that was used for identifying the attacks on the AMI were: (1) The commonality of the attacks that are being employed by the hackers, and the (2) severity of the attacks can cause the AMI.

Each chosen article was studied to determine if it achieved any of the following goals to discover the cybersecurity issues present in Smart Meters. The results of finding notorious attacks and their effects are presented in the results and discussions.

Distinguishing Cybersecurity requirements and solutions/defenses that counters the attack methods in Smart Meters in AMI

The criteria that was used for identifying the defenses on the AMI were: (1) The defenses that are employed in Smart Grids, and the (2) current innovations against attacks.

Reading each article helped the paper to pinpoint the cybersecurity problems impacting the Smart Meter and the AMI, as well as the remedies. The chosen articles had material that suggested remedies for the problems that were noted. These articles were to assess, debate, and evaluate the tools, frameworks, methods, and technologies that may be applied to address the highlighted problems.

Highlighting best solutions and defenses for identified Smart Meter in AMI Cybersecurity issues

The papers that addressed how to overcome the cybersecurity issues regarding smart meters were further examined to discover the most optimal and practical solutions. In order to compare the solutions, certain features that may be utilized to compare the solutions were identified after reading the gathered material. The attacks they can defend from, the positive results from the trials linked to them, and the disadvantages experienced while employing the solution are specified for comparing the solutions. The countermeasure that defends more attacks can be deemed efficient and can be implemented.

RESULTS AND DISCUSSION

This section illustrates an overview of the common attacks that have been employed against the AMI. This section also provides the description of the attacks and how serious it is for the AMI.

Majority of the studies (Jamal et. al. 2018; Alfassa et. al, 2021; Haider et. al, 2019; Tonyali et. al., 2017; Naseer et. al., 2021; Alsharif et. al., 2019; Sanjab et. al, 2016) et have highlighted that the most common attack and has the most severe effect on the smart grid is the Denial of Service, which is present in Table 1. Other attacks that are present are Eavesdropping/Sniffing, False Data Injection, Remote Connect/Disconnect, Firmware Manipulation, Man-in-the-Middle (MITM) and Power Hijacking.

Smart Meters in AMI Cybersecurity threats

Twenty publications were chosen for the literature review to address the first research question to pinpoint cybersecurity problems connected to AMI's Smart Meters. The papers used to discuss the cyberattacks are listed in Table 1.

Table 1:The Cybersecurity Threats of Smart Meters in AMI

Cybersecurity Attacks in Smart Meters in AMI	Articles
Eavesdropping/Sniffing	Ibrahem et. al, 2020; Saxena et. al, 2017; Alfassa et. al, 2021
Denial of Service	Jamal et. al. 2018; Alfassa et. al, 2021; Haider et. al, 2019; Tonyali et. al., 2017; Naseer et. al., 2021; Alsharif et. al., 2019; Sanjab et. al, 2016
Packet Injection/False Data Injection	Lee et. al., 2019; Chekired et. al., 2019; Kallitsis et. al., 2018; Unsal et. al., 2021; Haider et. al., 2019; Sanjab et. al., 2016
Remote Connect/Disconnect	Jakaria et. al., 2019; Tonyali et. al., 2017; Aljohani, 2022
Firmware Manipulation	Tonyali et. al., 2017
Man-in-the-Middle	Kulkarni et. al., 2020; Haider et. al, 2019; Sahu et. al., 2017

Power Hijacking	Singh et. al., 2017; Khan et. al., 2020;

Seven of the 20 papers addressed how Smart Meters are susceptible to Denial of Service (DoS). Six articles covered packet injection and false data injection after the DoS. Man-in-the-Middle attacks and eavesdropping/sniffing were covered in 3 publications. Three articles describe remote connect/disconnect, two studies discuss power hijacking, and firmware manipulation has one, and the following sections go into further detail on each of the problems as mentioned above.

Eavesdropping/Sniffing.

One of the issues of Smart Meters in the AMIs in general is the unauthorized monitoring and tracking of the target's power consumption and customer data (Ibrahem et. al, 2020). The study made by Alfassa et. al (2021) has indicated that some versions of smart meters have unencrypted data that is being passed through from the consumer to the service provider, allowing hackers to read the data that is being sent across the network. When a hacker eavesdrops on smart meters, they can determine whether or not there are people inside the house based from the Watts that are being recorded (Ibrahem et. al, 2020; Alfassa et. al, 2021). The hackers can also resend previous meter readings and can reveal the names and the location of the consumer (Saxena et. al, 2017).

Denial of Service

The forcible denial of service, or in this case, denial of power, is the most obvious attack that can be carried out against an AMI and a Smart Meter. Since DoS attacks not just the AMI and Smart Meters but also every device on the Smart Grid (Jamal et. al. 2018; Alfassa et. al, 2021; Haider et. al, 2019). Haider (2019) outlines how the assault in AMI and smart meters is referred to as a puppet attack. Depending on their preferences, any node or meter can be used by the attacker or hacker as their base or puppet. As soon as this puppet node or puppet meter receives malicious packets, it will flood other nodes or meters in the grid to overwhelm their communication (Sanjab et. al, 2016), which would eventually cause localized blackouts in some areas of the smart grid and result in a Distributed Denial of Service attack.

Packet Injection/False Data Injection

Five distinct literary works have referenced this specific incident. False Data Injection Attacks, or FDIAs, are intended to "inject malicious software and change numerous file systems," according to Unsal et. al, (2021) & Haider et. al, (2019). FDIA compromises the data integrity of smart meters, for instance, modifying the customer's information. This attack's primary goal is to compromise many AMI and smart meters sensors to alter the data and deceive the smart grid's decision-making mechanism. The capacity of FDIA to alter stored values makes it one of the most destructive forms of attacks among those listed above, according to Kallitsis et. al, (2018), Unsal et. al, (2021), & Haider et. al, 2019. FDIA has also been divided into three sub-categories (Haider et. al, 2019). The first is an economic assault FDI, which tries to alter the readings so that the user would pay more or less for their power. The Load Distribution Attack FDI falls under the second type and seeks to either over- or underload a customer's power load. The Energy Deceiving Attack, which hides a customer's true power use, comes last (Haider et. al, 2019).

Remote Connect/Disconnect

Because of built-in functionality, energy distributors and suppliers can remotely connect or disconnect a customer's power line in response to unpaid invoices (Jakaria et. al., 2019). According to Jakaria et. al. (2019) and Tonyali et. al., (2017) hackers can take advantage of this weakness by using or breaking into the network to install malicious software on the AMI and smart meters. Following this, the hacker can gather data like the IP addresses of other smart meters and send remote disconnect commands to the other smart meters. The Russian-Ukrainian war is presently seeing both sides use this specific attack (Aljohani, 2022).

Firmware Manipulation

Firmware manipulation is done by masking the attack as a legitimate firmware update. As stated by Tonyali et. al., (2017), these firmware update processes are used by smart meter vendors or the service providers. Usually, these providers notify users that an update is available, but hackers have found a way to exploit this to let them install their own programs in smart meters. Once their firmware is installed on the smart meters, it can enable hackers to enter or penetrate the whole smart grid without being detected.

Man-in-the-Middle

The term "Man-in-the-Middle," or MITM, is used to describe "stealing or modifying the data, i.e., intercepting communications or inserting new messages while the two parties interact" Kulkarni et. al. (2020). To explain, a

MITM attacker places himself between the service provider and the smart meter (Haider et. al, 2019 & Sahu et. al., 2017) and covertly modifies the communications between the two who are engaging. MITM tricks both the smart meter and the service provider into thinking that both are the legitimate end users of their communication.

Table 2: Attacks and Countermeasures

Countermeasure	Sniffing	DoS	False Data Injection	Remote Connect/ Disconnect	Firmware Manipulation	Man-in-the-Middle	Power Hijacking
Data Encryption (Ibrahem et. al, 2020; Saxena et. al, 2017, Alsharif et. al., 2019)	✓				✓	✓	
Authentication (Lee et. al, 2019; Naseer et. al., 2021; Naseer et. al., 2020)		✓	✓	✓	✓		✓
Intrusion Detection System (Chekired et. al, 2019; Jakaria et. al., 2019; Huang, 2021; Yao et. al., 2021; Park et. al., 2018; Sun et. al., 2020)		✓	✓		✓	✓	✓

Power Hijacking

Power hijacking's main objective is to steal power through the compromised smart meters and transmit false readings to the control center (Singh et. al., 2017 & Khan et. al., 2020). The use of electricity without the service provider's consent is another definition of power hijacking (Khan et. al., 2020). The bypassing of smart meters, stealing energy from unregistered users, falsifying meter readings, and direct connection from the main power line are all examples of power hijacking (Khan et. al., 2020).

The Cybersecurity defense against the security threats to Smart Meters

This section focuses on prominent countermeasures implemented in the smart grid, particularly for smart meters in the AMI, supported by relevant literature. The evaluation criteria for identifying effective defenses against threats include the number of successfully repelled attacks and the overall effectiveness of the defense strategies. Among the commonly cited countermeasures across 11 studies are Data Encryption, Authentication, and Intrusion Detection Systems, as detailed in Table 2.

Data Encryption

Protecting the confidential information stored in the AMI's Smart Meters is crucial. As a result, data must always be safe when it is being kept and transferred. Encryption can stop unauthorized parties from accessing and altering data. Smart Meters can be shielded from attacks like MITM and data sniffing through encryption. Ibrahem et al. (2020) presented Privacy-Preserving Monitoring and Billing Scheme Based on Functional Encryption, or PMBFE for short, as a safe method for energy billing and smart meter monitoring. Based on a unique form of public-key cryptography, functional encryption enables the secret-key holder to learn a function's output using encrypted input data without having access to it.

The study has also found out that the sniffer/eavesdropper that is able to intercept the readings will definitely learn nothing about their target because the Smart Meters will encrypt the readings using Functional Encryption, and therefore the attacker cannot safely decrypt the reading because they do not know the secret key needed to unlock said data. An additional homomorphic encryption and proxy re-encryption method is introduced by Saxena, Choi, and Grijalva (2017), which is safe and privacy-preserving. The approach may aggregate metering data without disclosing the accurate individual data (identification or energy use) to any third party, making it resistant to identity and data theft. Since electricity service providers should have the ability to access multiple Smart Meters at the same time securely, Alsharif, Nabil, Mahmoud, and Abdalla (2019) have presented EPDA, or the Efficient and Privacy-Preserving Data Collection and Access Control Scheme for Multi-Recipient AMI Networks to guarantee the simultaneous access of Smart Meters by authorized parties.

Authentication

The verification and authentication of the primary source of the data is also crucial to protect the data that is being sent from the Smart Meter into the AMI. Smart Meters need authentication when establishing a node-to-node communication (Lee et. al, 2019). Authentication can help fend off attacks that specifically impersonates an electricity service provider that can broadcast remote disconnect messages to different Smart Meters or they can impersonate a Smart Meter and send malicious code to the AMI and can directly affect the Smart Grid as a whole (Alfassa et. al, 2021). A unified strategy for power reading signal reduction and authentication in AMI is proposed by Lee, Hwang, and Choi (2019) and is based on compressive sensing. The aggregated power reading signal is efficiently authenticated using decompression.

For Smart Meters in AMI, Naseer, Bhutta, and Alojail (2020) have also suggested a Public Key based Key Transport protocol. Meters are linked to the smart grid through the Public Key Infrastructure (PKI)-based key exchange protocol, which also ensures that the Certificate Authority (CA) is always accessible (Naseer et. al., 2020). Blockchain technology is a new and innovative method of authenticating sent data Naseer et. al., 2021. A lightweight control access system that authenticates smart meters and enrolls them securely in the network has been integrated by Naseer, Ullah, and Anjum Naseer et. al., 2021.

Intrusion Detection System

Intrusion Detection Systems (IDS), such as the HD-IDS proposed by Chekired, Khoukhi, and Mouftah (2019), play a vital role in monitoring and securing data and communications within AMIs. Their HD-IDS employs a distributed fog architecture, encompassing home area networks, residential area networks, and fog operations center networks, with a focus on identifying and resolving issues through stochastic modeling based on the Markov Chain Process. Additionally, Jakaria, Rahman, and Moula (2019) highlight the applicability of both supervised and unsupervised machine learning methods to identify questionable data for safeguarding Smart Meters and AMIs.

Machine learning algorithms enhance smart meter security by identifying suspicious nodes and detecting data alteration (Jakaria et al., 2019). Huang (2021) applies machine learning in Forest Management and Resource Monitoring, supplementing outdated detection mechanisms in Smart Meters and AMIs. Yao et al. (2021) propose a CNN-LSTM model for intrusion detection in AMIs, demonstrating its superiority over traditional ML algorithms for ensuring communication security among Smart Meters. The success of machine learning-based intrusion detection, as observed in Park, Li, and Hong's (2018) study, is attributed to higher anomaly detection rates compared to older systems.

Additional suggested countermeasures for the identified attacks in AMIs, particularly in Smart Meters

In general, advanced modern encryption, machine learning, and blockchain have been the most significant methods of preventing attacks to the AMI, especially in Smart Meters. Data encryption should always be enforced with advanced modern cryptography standards. Blockchain is useful for authentication, whereas machine learning is better suited for intrusion detection systems.

Advanced Modern Cryptography

To counter Eavesdropping/Sniffing, Firmware Manipulation, and MITM attacks, advanced modern cryptography, like EPDA, stands out by allowing computational processes without the need to decrypt data first, preserving its privacy (Alsharif et al., 2019).

Blockchain

Blockchain's decentralized nature seamlessly integrates with the AMI system, distributing administration across devices like smart meters. This eliminates reliance on a central authority, enhancing security. Smart meters, as end devices, gain the ability to detect and counteract suspicious commands, bolstering authentication procedures (Naseer et al., 2021). This decentralization makes it harder for attackers to breach the system.

Machine Learning

With ICT integrated into the Smart Grid, it introduces a whole lot of information to conventional grids.

Machine learning and big data analytics should enable huge collection of data in the grid that can create value for the service provider. ML can provide information such as load forecasting and load analysis, which is useful for an IDS, as mentioned by Jakaria, Rahman, and Moula (2019), and in Yao, Wang, Liu, Chen, and Sheng (2021), as it can autonomously analyze gaps and inconsistencies in the network itself. Traditional problems such as analyzing logs, tracing packets, and studying system events are solved via machine learning.

CONCLUSION

This paper provides a survey of Smart Meters in AMI security, which shows the attacks and defenses currently being employed in the industry. To glimpse what Smart Meter in AMI security is, here is a brief discussion of the current security issues that are being faced. The security issues being faced by Smart Meters in AMIs are eavesdropping, Denial of Service (DoS), False Data Injection (FDI), Remote Connect/Disconnect, Firmware Manipulation, Man-in-the-Middle (MITM), and Power Hijacking.

Along with the cybersecurity issues, proposed defenses were also identified. The majority of the securities address a multitude of attacks that are present in Smart Grids. The articles that were identified as defenses were grouped into three categories, Data Encryption, Authentication, and Intrusion Detection Systems. Sniffing and MITM attacks can be thwarted by using data encryption methods. DoS, FDIs, Remote Connect/Disconnect, Firmware Manipulation, and Power Hijacking can be defended by rigorous authentication methods. DoS, FDIs, Firmware Manipulation, MITMs, and Power Hijacking can also be monitored and countered by an Intrusion Detection System.

The articles presented were compared in each category and identified the better defense overall. Advanced Modern Cryptography was identified as the best way to address the attacks such as eavesdropping/sniffing and MITM. Blockchain as a way to authenticate verified nodes in the system is also the best way to thwart attacks focused on DoS, FDI, Remote Connect/Disconnect, Firmware Manipulation, and Power Hijacking. Finally, Machine Learning can further block attacks by having an autonomous system that decides whether the processes or actions being done in the system are legitimate, thus creating value for electricity service providers.

ACKNOWLEDGEMENTS

The corresponding author would like to thank Dr. Gerry Paul Genove for his guidance and advice for the paper and would also like to thank the support of the DOST-STRAND Scholarship. To my parents, thank you as well.

REFERENCES

Alfassa, S. M., Nagasundari, S., & Honnavalli, P. B. (2021). Invasion Analysis of Smart Meter In AMI System. *2021 IEEE Mysore Sub Section International Conference (MysuruCon)*. https://doi.org/10.1109/mysurucon52639.2021.9641595

Aljohani, T. M. (2022). Cyberattacks on Energy Infrastructures: Modern War Weapons. *ArXiv:2208.14225 [Cs]*. Retrieved from https://arxiv.org/abs/2208.14225

Alsharif, A., Nabil, M., Mahmoud, M. M. E. A., & Abdallah, M. (2019). EPDA: Efficient and Privacy-Preserving Data Collection and Access Control Scheme for Multi-Recipient AMI Networks. *IEEE Access, 7,* 27829–27845. doi.org/10.1109/access.2019.2900934

AVCI, İ. (2021). Investigation of Cyber-Attack Methods and Measures in Smart Grids. *Sakarya University Journal of Science*. doi.org/10.16984/saufenbilder.955914

Azad, S., Sabrina, F., & Wasimi, S. (2019, November 1). Transformation of Smart Grid using Machine Learning. https://doi.org/10.1109/AUPEC48547.2019.211809

Blakely, L., Reno, M. J., & Ashok, K. (2019, June 1). AMI Data Quality and Collection Method Considerations for Improving the Accuracy of Distribution Models. https://doi.org/10.1109/PVSC40753.2019.8981211

Chekired, D. A., Khoukhi, L., & Mouftah, H. T. (2019). Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. doi.org/10.1109/icc.2019.8761752

Fan, X., & Gong, G. (2013). Security Challenges in Smart-Grid Metering and Control Systems. *Technology Innovation Management Review*, *3*(7), 42–49. https://doi.org/10.22215/timreview/702

Ghelani, D. (2022). Cyber Security in Smart Grids, Threats, and Possible Solutions. *American Journal of Applied Scientific Research*.https://doi.org/10.22541/au.166385207.71655799/v1

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. (2021). *NIST framework and roadmap for smart grid interoperability standards, release 4.0*. https://doi.org/10.6028/nist.sp.1108r4

Haider, M. H., Saleem, S. B., Rafaqat, J., & Sabahat, N. (2019, December 1). Threat Modeling of Wireless Attacks on Advanced Metering Infrastructure. 10.1109/MACS48846.2019.9024779

Haq, E. U., Xu, H., Pan, L., & Khattak, M. I. (2017, August 1). Smart Grid Security: Threats and Solutions. doi.org/10.1109/SKG.2017.00039

Huang, C. (2021). Forest management and resource monitoring based on AMI intrusion detection algorithm and artificial intelligence. *Journal of Ambient Intelligence and Humanized Computing*. doi.org/10.1007/s12652-021 03211-y

Ibrahem, M. I., Badr, M. M., Fouda, M. M., Mahmoud, M., Alasmary, W., & Fadlullah, Z. Md. (2020). PMBFE: Efficient and Privacy-Preserving Monitoring and Billing Using Functional Encryption for AMI Networks. *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. https://doi.org/10.1109/isncc49221.2020.9297246

Jakaria, A. H. M., Rahman, M. A., & Moula Mehedi Hasan, M. G. (2019). Safety Analysis of AMI Networks Through Smart Fraud Detection. *2019 IEEE Conference on Communications and Network Security (CNS)*. doi.org/10.1109/cns.2019.8802845

Jamal, T., Haider, Z., Butt, S. A., & Chohan, A. (2018). Denial of Service Attack in Cooperative Networks. *ArXiv:1810.11070 [Cs]*. Retrieved from https://arxiv.org/abs/1810.11070

Kallitsis, M. G., Bhattacharya, S., & Michailidis, G. (2018, October 1). Detection of False Data Injection Attacks in Smart Grids Based on Forecasts. https://doi.org/10.1109/SmartGridComm.2018.8587473

Kawoosa, A. I., & Prashar, D. (2021). A Review of Cyber Securities in Smart Grid Technology. *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*. https://doi.org/10.1109/iccakm50778.2021.9357698

Khan, Z. A., Adil, M., Javaid, N., Saqib, M. N., Shafiq, M., & Choi, J.-G. (2020). Electricity Theft Detection Using Supervised Learning Techniques on Smart Meter Data. *Sustainability*, *12*(19), 8023. https://doi.org/10.3390/su12198023

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. doi.org/10.1016/j.ijcip.2019.01.001

Kulkarni, S., Rahul, R. K., Shreyas, R., Nagasundari, S., & Honnavalli, P. B. (2020). MITM Intrusion Analysis for Advanced Metering Infrastructure Communication in a Smart Grid Environment. *Communications in Computer and Information Science*, 256–267. https://doi.org/10.1007/978-3-030-66763-4_22

Lee, C., Yang, H., Lee, B., & Won, D. (2012). A Novel Privacy-Enhanced AMI System Using Searchable and Homomorphic Encryption Techniques. *Convergence and Hybrid Information Technology*, 608–617. https://doi.org/10.1007/978-3-642-32645-5_76

Lee, Y., Hwang, E., & Choi, J. (2019). A Unified Approach for Compression and Authentication of Smart Meter Reading in AMI. *IEEE Access*, *7*, 34383–34394. doi.org/10.1109/access.2019.2903574

Mrabet, Z. E., Kaabouch, N., Ghazi, H. E., & Ghazi, H. E. (2018). Cyber-security in smart grid: Survey and challenges. *Computers & Electrical Engineering*, *67*, 469–482.doi.org/10.1016 /j.compeleceng.2018.01.015

Naseer, H., Mumtaz Bhutta, M. N., & Alojail, M. A. (2020, October 1). A Key Transport Protocol for Advance Metering Infrastructure (AMI) Based on Public Key Cryptography. https://doi.org/10.1109/ICCWS48432.2020.9292385

Naseer, O., Ullah, S., & Anjum, L. (2021). Blockchain-Based Decentralized Lightweight Control Access Scheme for Smart Grids. *Arabian Journal for Science and Engineering*. doi.org/10.1007/s13369-021-05446-5

Otuoze, A. O., Mustafa, M. W., & Larik, R. M. (2018). Smart grids security challenges: Classification by sources of threats. *Journal of Electrical Systems and Information Technology*, *5*(3), 468–483. https://doi.org/10.1016/j.jesit.2018.01.001

Park, S.-T., Li, G., & Hong, J.-C. (2018). A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. *Journal of Ambient Intelligence and Humanized Computing*, *11*(4), 1405–1412. https://doi.org/10.1007/s12652-018-0998-6

Parvez, I., Sarwat, A., Wei, L., & Sundararajan, A. (2016). Securing Metering Infrastructure of Smart Grid: A Machine Learning and Localization Based Key Management Approach. *Energies*, *9*(9), 691. https://doi.org/10.3390/en9090691

Philips, A., Jayakumar, J., & Lydia, M. (2020). A Review on Cyber Security in Metering Infrastructure of Smart Grids. *Computational Methods and Data Engineering*, 117–132. https://doi.org/10.1007/978-981-15-6876-3_10

Rothstein, H. R. (2012). Accessing relevant literature. *APA Handbook of Research Methods in Psychology, Vol 1: Foundations, Planning, Measures, and Psychometrics.*, 133–144. https://doi.org/10.1037/13619-009

Sahu, A., Tippanaboyana, H. N. R. K., Hefton, L., & Goulart, A. (2017, September 1). Detection of rogue nodes in AMI networks. doi.org/10.1109/ISAP.2017.8071424

Sanjab, A., Saad, W., Guvenc, I., Sarwat, A., & Biswas, S. (2016). *Smart Grid Security: Threats, Challenges, and Solutions*. Retrieved from https://arxiv.org/pdf/1606.06992.pdf

Saxena, N., Choi, B. J., & Grijalva, S. (2017). Secure and privacy-preserving concentration of metering data in AMI networks. *2017 IEEE International Conference on Communications (ICC)*. doi.org/10.1109/icc.2017.7996874

Singh, S. K., Bose, R., & Joshi, A. (2017). Entropy-based electricity theft detection in AMI network. *IET Cyber-Physical Systems: Theory & Applications*, *3*(2), 99–105. https://doi.org/10.1049/iet-cps.2017.0063

Subramaniam, T. (2022, November 15). Global population hits 8 billion as growth poses more challenges for the planet. Retrieved from CNN website: https://edition.cnn.com/2022/11/15/world/global-population-8-billion-un-intl-hnk/index.html

Sun, C.-C., Sebastian, D. J., Hahn, A., & Liu, C.-C. (2020). Intrusion Detection for Cybersecurity of Smart Meters. *IEEE Transactions on Smart Grid*, 1–1. doi.org/10.1109/tsg.2020.3010230

Tonyali, S., Akkaya, K., Saputro, N., & Cheng, X. (2017, July 1). An Attribute & Network Coding-Based Secure Multicast Protocol for Firmware Updates in Smart Grid AMI Networks. https://doi.org/10.1109/ICCCN.2017.8038415

Unsal, D. B., Ustun, T. S., Hussain, S. M. S., & Onen, A. (2021). Enhancing Cybersecurity in Smart Grids: False Data Injection and Its Mitigation. *Energies*, *14*(9), 2657. https://doi.org/10.3390/en14092657

Waters, G. (n.d.). Conquering Advanced Metering Cost and Risk. Retrieved November 23, 2022, from Electric Energy Online website: https://electricenergyonline.com/show_article.php?article=297

Yao, R., Wang, N., Liu, Z., Chen, P., & Sheng, X. (2021). Intrusion Detection System in the Advanced Metering Infrastructure: A Cross-Layer Feature-Fusion CNN-LSTM-Based Approach. *Sensors*, *21*(2), 626. https://doi.org/10.3390/s21020626

NAME: GIAN LLOYD JACOBA
CONTACT NO: 09988589517
EMAIL ADDRESS: gljacoba@protonmail.com