Ajiboye *et al.*
Journal of Engineering and Applied Science (2024) 71:91
https://doi.org/10.1186/s44147-024-00422-w

Journal of Engineering and Applied Science

REVIEWS **Open Access**

Privacy and security of advanced metering infrastructure (AMI) data and network: a comprehensive review

Priscilla Oyeladun Ajiboye[1*], Kwame Opuni-Boachie Obour Agyekum[2] and Emmanuel Asuming Frimpong[1]

*Correspondence:
oyeladpri@gmail.com

[1] Department of Electrical and Electronic Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
[2] Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Abstract

The traditional electrical grid has to be digitally improved as digitalization and effective integration of renewable energy bring better efficiency, intelligence, and safety into the grid; hence, the transition from the traditional grid to a smart grid. A smart grid is a modernized and digitalized standard electrical infrastructure that has a key component known as the advanced metering infrastructure (AMI). AMI, also known as smart metering, is a key technological enabler of the smart grid that allows automatic collection and reporting of power-consumed data via two-way communication networks. However, the collected power consumption data is confidential; hence, its privacy must be maintained. Similarly, for the benefit of the smart grid to be consistently maximized, the AMI data and network security must always be intact despite the evolving threats and attacks targeted at it.

This paper provides a comprehensive review of the existing vulnerabilities/attacks, security and privacy challenges associated with the smart metering data and network system, its open issues, and future direction. The major contributions of this review paper lie in the AMI vulnerabilities, AMI state-of-the-art security schemes with their pros and cons, its communication protocols analysis, and its emerging security measures. This gave enumerated recommendations for the efficiency improvement of AMI security in terms of its latency reduction while implementing efficient security measures in its future work.

Keywords: Advanced metering infrastructure, Communication protocol, Data/network security, Countermeasures, Vulnerabilities

Introduction

Smart grid (SG) is an electrical power system with scalable, pervasive two-way communications and timely control capabilities. It is also known as the future power infrastructure of the energy world due to the smart attributes introduced by its major component; the advanced metering infrastructure (AMI). The AMI accommodates several consumers and devices within different types of networks and several endpoints in the distribution system. It is therefore regarded as a complex network that comes with various security threats and issues due to its large data management and integration with information communication technology (ICT) [1, 2].

© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/. The Creative Commons Public Domain Dedication waiver (http://creativecommons.org/publicdomain/zero/1.0/) applies to the data made available in this article, unless otherwise stated in a credit line to the data.

Springer Open

Also, consumers' data are collected, measured, and reported to the utility center in real-time by the smart meters. This allows the optimization of the supplied and distributed electricity. Unfortunately, the collected customers'/users' data have been reported as a way of invading users' privacy by revealing individuals' household private information (like their economic status). This information can be used for criminal purposes [3, 4]. Hence, the AMI data and network are subjected to great security and privacy concerns.

Security is a controlling factor in AMI and it comes with three major objectives which are: Confidentiality of data, Integrity of shared information, and Availability of service (commonly known as CIA or AIC Triad) [1, 5]. The CIA triad ensures AMI safety (that is, the equipment safety, the safety of the system certification, and the safety of communicated data) via different security processes such as preventing equipment tampering, unauthorized data access and forgery through encryption, firewalls, authentication and other valid means [6].

However, there have been several studies on the aforementioned AMI security and privacy issues. This is because a nation's security and economy alongside her public safety largely rely on it [7]. More so, its failure or inadequacies have been found to have debilitating impacts such as huge economic and property losses as experienced in 2003 when the United States of America (USA) blackout caused billions of dollars; which is also an example of similar security breach experiences in other nations [6].

Many recent articles have surveyed either one or both the security and privacy problems in AMI, to solve the associated problems of threats and attacks. For better clarity in this review, AMI system security, AMI data privacy, and AMI network security will be reviewed and thoroughly analyzed.

The remaining parts of this paper are as follows. Section 2 is divided into sub-sections and it gives a review of some existing techniques for securing AMI, privacy and security vulnerabilities of AMI, data privacy of AMI, network security of AMI, AMI overview and components, AMI architecture and its communication protocols, vulnerabilities, and countermeasure techniques. Sub-sections 2 ends with open issues/future research. The paper concludes at Section 3.

Existing review papers on AMI security

According to Alfassa et al. [7], a brief introduction of smart grid, AMI, and its communication networks with diagrams, alongside the requirements of network privacy and security in smart metering were stated. The study analyzed the potential security issues introduced by man-in-the-middle (MiTM) attacks and session hijacking attacks. Also, countermeasures for the attacks and vulnerabilities, limiting the functional cookies on the web servers to prevent the attacker from gaining access into the system are discussed.

Different uses of AMI data, privacy policies, and privacy-preserving technologies in the areas of billing, operations, and demand response as surveyed in papers from 2009 to 2016 were presented without the security challenge [3]. The paper explained the various uses of metering data and corresponding privacy legislation, compared the attacks on the traditional grid with the ones targeted at the smart grid AMI, and derived some privacy requirements for smart metering with no real emphasis made on open research issues in AMI. The review further explained past studies in the area of privacy-preserving techniques under three (3) groups. These groups were: value-added services, billing, and operations. Identification of interception, denial of service (DOS), and MiTM as the major forms of attack targeted at AMI with lightweight cryptosystem as an open issue for its security was done [8]. The paper left out some other possible attacks that can also collapse the grid via AMI attack. Ur-Rehman, N. Zivic, and C. Ruland focussed more on the security and privacy of AMI system, listed some smart metering potential attackers based on the 2010 to 2014 surveyed papers and a security by design approach known as "Trusted Computing Engineering for Resource Constraint Embedded Systems Application" was presented for its security [9].

A. Anzalchi and A. Sarwat assessed the security requirements of AMI, the vulnerability of the network, and countermeasures for the various attacks and studied some authentication techniques that exist between smart meters and the utility centers and their importance [10]. The paper further considered the AMI security problem from 3 perspectives. These were: the maintenance of customers' data privacy and the durability of the system against several attacks and power theft. Its countermeasures were access control and security of protocols (in terms of explicit names, unique encoding, and usage of timestamps). M. Shokry et al. presented a systematic survey of AMI security from different areas such as the attacks, countermeasures, and open research [11]. The paper's uniqueness was identified to be comprehensive of different attacks on specific vulnerabilities of each AMI component and the system at large. Also, the impacts of the mentioned attacks on each of the components and the overall system as well were discussed.

Kayalvizhy and Banumathi [4] centered more on temporary thoughts of cyber-attack operations in AMI, the attacks against the AMI hardware layer (the smart meters), and their corresponding mitigation methods. Moreover, based on previously reviewed threat and attack models, different proposals for threat mitigation were also made by the authors. Some threats to AMI security and privacy that were listed include; smart meter impersonation, meter module interloping, change of meter location, and unauthorized interruption on transmission channels [12]. indicated to be the first survey to enumerate the importance of key management system (KMS) in AMI security. The survey stated the key management techniques for securing AMI from vulnerable attacks to be; key graph, physically unclonable function (PUF) based, encryption-based, and hybrid (involving symmetric and asymmetric) techniques. It also differentiated the traditional electrical power systems from the smart grid. In addition, the survey highlighted AMI security challenges as privacy preservation of end users, AMI system durability against attacks, and prevention of power theft.

Desai et al. [13] explained the privacy problems associated with AMI data and also some corresponding solutions with future research directions. The paper gave 2 types of data that are transmitted by smart meters based on data attacks. These were power consumption values and smart meter readings at an exact time and location. It further recommended safety mechanisms such as firewall, digital signature, access control, trusted platform, and encryption for the prevention of data theft in AMI. Mrabet et al. [14] discussed the CIA triad as the basic AMI security requirements, classified some attacks targeted at the AMI to be MiTM, replay, DOS, CIA triad violation, and virus/worms/trojan horse attacks, and a cyber-security technique made up of three (3) phases as a corresponding countermeasure to the attacks. These phases were pre-attack, under-attack, and post-attack phases with each phase accompanied by security protocols, cryptography, and some other countermeasures.

Pedramnia and Rahmani [15] discussed the long-term evolution (LTE) vulnerabilities that end up in indifferent DOS attacks, the pathways to the attack, and corresponding countermeasures for these attacks' detection. Signaling DOS, jamming, short message service (SMS) link saturation, attack request, and traffic flooding were listed as the types of DOS attacks, and machine learning techniques, firewalls, and spread spectrum transmission were the proposed countermeasures for the mentioned DOS attacks.

Hansen et al. [16] discussed the security challenges in AMI comprising over one (1) million smart meters, over one hundred data collectors, and a 2-m data management system (MDMS). It identified eight (8) attack vectors as the attack surface of AMI. These attack vectors include physical and cyber access to the internals of smart meters and that of the data collector through different means such as through the technician's tools or a trade-off supply chain. The paper also discussed the impacts of attacks launched via the 8 attack vectors as data and power thefts, power denial, and the entire grid disruption. The results from this paper were said to be a foundation for creating a risk management program for attack mitigations.

Tan et al. [17] reviewed different security challenges in AMI via a data-driven approach. The paper focussed more on vulnerabilities, attacks, and solutions which were broken down into 4 stages of data: generation, acquisition, storage, and processing. Data analytics was also used by the authors for the smart grid-AMI security analytics. Tong et al. [18] examined the state-of-the-art methods in the application of intrusion detection systems (IDS) for AMI security and further described different types of IDS as security measures for AMI systems. These include specification-based (network identity (ID) and host ID) and anomaly-based IDS. End devices and communication networks were identified here as the attack surfaces for AMI. The study was concluded with a proposed comprehensive distributed IDS for AMI security. Jokar et al. [19] gave a detailed explanation of different cyber-attacks on the smart grid; with emphasis on those attacks that affect AMI data privacy. Monitoring in IDS, key management systems in cryptography, security threats, and data privacy were identified as the major challenges facing AMI security [20].

Chris Foreman and Gurugubelli [21] discussed the prominent surfaces of the AMI components that are vulnerable to cyber-attacks for the software, hardware, protocols, and network configurations. Grid disruption, power denial, and theft were identified as the major targeted attacks in this paper while the AMI attack surfaces were smart meters, communication networks, smart meters data collectors, protocols, and software. Rashed Mohassel et al. [22] introduced AMI as the smart grid's major foundation, established the relationship between them, and discussed the security issues of AMI based on identified AMI's three (3) subsystems. These were: AMI smart devices, communication, and data management systems. It also considered some major attacks that can be targeted at a home area network together with other smart components in AMI such as the smart meters.

Ancillotti et al. [23] proposed two (2) major communication sub-systems for AMI. These were a communication infrastructure and a middleware platform. It further recommended physical protection of the devices alongside physical isolation of utility control centers based on the reviewed safety measures for the communication means. Na et al. [24] and Tyav et al. [25] further highlighted and investigated vulnerabilities and common attacks such as the false data injection (FDI) attack and MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK), which can collapse the grid by attacking the AMI components. The paper also discussed data communication security via cryptography.

Considering past reviews, no previous review regarding the privacy and security challenges of AMI has investigated AMI data communication protocol for the security improvement of AMI, and its latency reduction alongside its possible future work. This demonstrates the significance and the need for this survey which specifically identifies past security breaches of the AMI system, its communication protocols' vulnerabilities, the impact of the vulnerabilities, and related future work for improving security with less accompanying delay, apart from the other reviews done.

Existing techniques/approaches for securing AMI

Considering various existing proposed schemes for controlling and mitigating AMI attacks and security compromise, different approaches have been employed in achieving this, but not without their pros and cons. Some of these approaches are physically Unclonable functions (PUF), artificial intelligence (AI), blockchain, classical cryptography (CC), quantum encryption (QE), and post-quantum cryptography (PQC). Table 1 further summarizes each of these schemes with their pros and cons.

Privacy and security vulnerabilities of AMI

AMI is an automated two-way communication structure that gathers metering information in utility set-up to improve the smart grid operations and the quality of power service received by customers [11]. Its data storage and communication method make the AMI system more vulnerable to different threats and cyber-physical attacks which require adequate and efficient security countermeasures. In achieving this, the major security objectives include CIA or AIC Triad) [1, 5].

Confidentiality in AMI implies that data/information (such as the customers' power consumption details and the customers' personal details) cannot be accessed by un-authorized users. Its integrity involves there are no modification(s) of the sent and received data from the utility center to the customers and vice versa, while service availability is best defined as the time percentage that a steady service is made available to the customer [37].

In achieving the security objectives of AMI, several authors have studied different techniques to ensure a better AMI security without exchanging latency for security or vice versa. Some of these techniques include blockchain, cloud computing, and general cryptographic techniques as earlier mentioned. Robles et al. [38] combined the building features of blockchain technology to initiate and utilize a customer-focused data management system in AMI. Since blockchain is a decentralized public digital ledger for recording transactions that cannot be changed without changing all the subsequent blocks and the consensus of the network, access control, integrity, and authentication of the involved data were therefore guaranteed via blockchain [39, 40]. Blockchain's

Table 1 Tabular representation of some existing AMI security techniques with their pros and cons

S/N	AMI security techniques	Pros	Cons
1	Physically Unclonable functions (PUF)	A good AMI security technique with relatively low computational and communication overhead [26]	PUFs get easily denatured/altered in the presence of extreme temperatures [27]
2	Blockchain technique	Blockchain addresses several security challenges surrounding traceability, authentication, scalability, and data privacy in AMI better than techniques like the PUF that address fewer challenges per time [28].	Blockchain security schemes introduce relatively higher delays to systems and are usually not quantum-resistant [29]
3	Artificial intelligence (AI) technique	Relatively fast and accurate anomaly detection rates [30]	Mostly deployed for the detection of threats and attacks [31]
4	Quantum encryption (QE) technique	It is a quantum-resistant technique with efficient security [32]	Its implementation involves complicated processes with many constraints to be resolved in its practical application [33]
5	Post-quantum cryptography (PQC), e.g., lattice-based cryptography	A good security technique for AMI; resistant against both quantum attacks	Introduces relatively more delay and higher computational complexity and communication overhead than classical cryptography techniques [34]
6	Classical cryptography (e.g., lightweight elliptic curve cryptography (ECC) scheme and its variants)	Mostly lightweight security techniques for maintaining the authentication, confidentiality, and integrity of AMI data [35].	Classical cryptography technique is not resistant to quantum attacks [36].

characteristic features and benefits of data storage, fraud protection, easy management, and ownership which involves security maintenance via keys and signatures, were harnessed for data management and security in [38]. This was achieved by initiating a scene where customers can utilize their keys for getting and translating cryptographic information accordingly.

However, the main challenge of blockchain adoption in [38] was in the provision of a public blockchain infrastructure in which ways of preventing read access to data in public networks were not available. Hence, the need for further complex cryptographic solutions to solve this problem was recommended.

Similarly, cloud computing, a process that enables the sharing of network resources (such as servers) with easy access via the internet, has been explored for AMI's larger data storage and security. This involves the utility center being located in the cloud instead of a physical utility center; though with limitations such as relative security and reliability, misconfiguration, limited flexibility and control, and downtime [41, 42]. Hence, better flexible, secured, and reliable techniques can be studied. Nevertheless, Brito et al. [43] emphasized on some advantages of cloud computing in AMI data security which were relative cost reduction, agile, and better self-service management. The study further leveraged on some Secure Cloud technologies such as Intel software guard extensions (SGX), OpenStack, and Kubernetes, to provide cloud platforms to run secure applications in ensuring the confidentiality and integrity of AMI data when running in a potentially untrusted cloud.

Data privacy of AMI

Privacy, though severally defined by different scholars; has been internationally defined by the United Nations (UN) as the assumption that everyone should have a self-governing area known as a "private sphere" that is not subjected to any uninvited intervention [44] expresses this as the ability of individuals to choose who has their information and what such information is used for. This privacy definition similarly applies to smart meters' data privacy.

According to a comparative analysis between data privacy and smart meters carried out by D. Lee and Hess [45], smart meters' ability to gather highly detailed information about the appliances in use over short intervals reveals the socio-economic status and other private information of such homes. This raises privacy concerns and security risks as attackers can make relatively accurate inferences on the ongoing activities in homes and also when no one is home. The comparative study presented four major implementation strategies for AMI data privacy policies to ensure that the integrated software (that is, the information communication technology (ICT)), consumption data and the digitalized electricity system do not lose public confidence [46].

Also, based on a combination of elliptic curve cryptography (ECC) with homomorphic encryption, [47] suggested a privacy-preserving data aggregation strategy; the ECBDA Scheme in which the AMI smart meter endorses its encrypted data before transmitting it to the aggregator which also confirms and aggregates the received messages without decrypting them. The aggregator in the same way endorses the received messages before transmitting them to the operation center. This privacy-preserving strategy was found to have advantages and disadvantages as stated in Table 2.

Similarly, Gough et al. [48] and Shateri et al. [49] proposed the differential privacy (DP) method as an efficient way of implementing data privacy in AMI smart meters. DP is a method in which information in two different datasets is compared in groups instead of comparing them with individuals. This ensures data privacy in the sense that individuals do not need to broadcast their private information and the power producers and energy retailers still have sufficient information to work with. In addition, the DP method involves the addition of noise to each consumer load profile to protect their privacy. This is done long before the comparison. However, DP ensures the privacy of datasets more than the privacy of individual data. Hence, it does not ensure absolute AMI data privacy; especially where the datasets are not very large enough to be difficult to trace and identify individuals' data [50].

Another technique of addressing data privacy in AMI, known as generative adversarial privacy (GAP) was studied by Shateri et al. [49]. The study revealed that GAP involves the use of a deep neural network (DNN) which targets minimizing an opponent's probable greatest loss when decisions made are dependent on the opponent's possible decisions. In AMI, this applies when GAP is used to add a minimal distortion in the form of noise to the transmitting data for the opponent/attacker to have the least accurate information about the smart meters' data.

Other techniques like anonymization of AMI data (Pseudonyms) for ensuring data privacy have also been studied by past researchers. Pseudonyms is a method involving 3rd party escrow technique for anonymous data collection in AMI [51].

The summary of the enumerated techniques with their corresponding pros and cons are tabularly represented in Table 2.

However, both analog meters and smart meters have privacy issues but their challenges differ as a result of their differences in volume, frequency and the detailed data gathered [45]. Moreover, the impacts of smart meters' data privacy concerns are experienced in various ways [52]. For example, it delayed the enabling legislation of smart meters in the Netherlands [53], and it was the third highest discussed concern across the United Kingdom (UK) media [54, 55], it led to public opposition against smart meters installation in France and North America [56]. Africa isn't left out as smart meters' high cost despite its privacy issues has limited its deployment to a large extent [57].

Network security of AMI

The AMI communication network provides a path for data and information flow within the AMI. Kayalvizhy and Banumathi [4] and Ngcobo and Ghayoor [58] explained its basic components as home area network (HAN), neighborhood area network (NAN), wide area network (WAN), and the customer gateway with each area network having a different data rate and coverage area that suits its functionality (Fig. 1).

The HAN

The HAN is a type of network present in a user's office or home. It is a communication medium for device interface sensors, relays, etc. It connects the user's energy monitoring device to a smart meter to facilitate the user's real-time energy usage monitoring. This helps in developing energy-saving habits and also in making informed decisions about a user's energy usage [59].

Table 2 Tabular representation of the pros and cons of some AMI data privacy techniques

Data privacy preserving technique	Pros	Cons	Remarks/recommendation
ECBDA Scheme	Supports multiple operations on encrypted data, is computationally efficient, performs well with a large number of consumers, and allows experimentation into losses and power quality issues.	Usually associated with latency, complex and slow performance with high storage requirements, it is not user-friendly	The homomorphic part of the scheme that introduces complexity can be replaced with lighter and more efficient computations
Differential privacy (DP)	Has cost and benefit analysis for consumers' flexibility in choosing an affordable plan, its billings are accurate, user-friendly, and easy to implement.	Does not ensure complete privacy, no protection against inference privacy, and greater energy loss is experienced here.	Its advantages make it easier to implement while ensuring trusted communications between the consumer and the data center
Generative adversarial privacy (GAP)	Protected against inference privacy, high accuracy and precision of data sent and received	Involves slow and complex training of the neural network which accounts for its high cost.	Suitable for big datasets with long-term memories
Pseudonyms	Its anonymity gives an edge relatively	Weak method, the possibility of tracing and matching up the anonymous to the right corresponding data is relatively high.	In addition to its anonymity, other encryption means can be hybridized with it for better security.

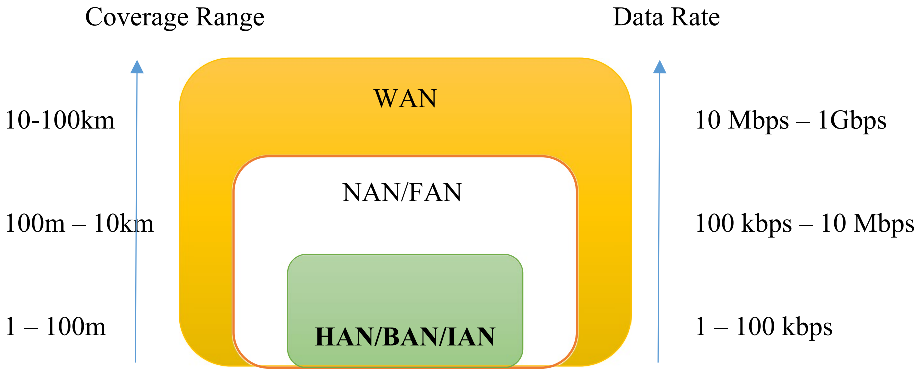

Fig. 1 AMI communication networks coverage range and data rate [4]

The WAN

The WAN gathers control and smart meters data/information and sends these readings to the server. It links the data concentrators (DCs) to the MDMS.

Customers' gateway

This is the channel between the AMI network and other smart devices within the customers' space. For example, the HAN, WAN, etc. as defined earlier. The customer domain consists of NAN (also known as field area network (FAN)) which connects the collector that sends data to the control at the utility center to the installed smart meters in homes, gateway, and the HAN.

Figure 1 shows each of the network's data rates and coverage area.

However, these networks are prone to several types of attack which can also affect the transmission of data and information; thereby, making both the data and network insecure. Some of these attacks include but are not limited to replay, spoofing, eavesdropping attacks, etc. Table 2 illustrates some network security vulnerabilities in AMI, their corresponding attacks, consequences, and countermeasures [60].

Despite one of the golden rules of cyber-physical security that: "a system risk is greater than the aggregate risk of its components because, the higher the number of its vulnerable components, the more difficult it becomes to trace the attacks"; identifying the possible attacks for the AMI components is still important [11, 61] (Table 3).

Past work done on AMI network security

A lightweight concealed-based security scheme (CBSS) as a secure network for communication/transmission in AMI was proposed [67]. This was achieved via the network simulator 2 environment together with direct encryption and decryption of any 2 arbitrary prime numbers. It also involved base stations, web servers, utility centers, customers, and smart meter nodes.

The scheme's prototype development was initiated when connection configuration was achieved (communication) between the utility center and the customers' smart meter with the nodes serving as interface. The smart meter was responsible for detecting and taking the readings (data) and sending it to the base station through multi-hop communication, which also sends it further to the gateway and then to the utility center where operations like the billing exercise take place before being sent back to the customer

Table 3 Security vulnerabilities in AMI network, their corresponding attacks, consequences, and countermeasures [62–66]

Year of publication	Targeted AMI component	Vulnerabilities	Related attacks	Attack consequences	Countermeasures
2020, 2017, 2013, 2019, 2012, 2016, 2018, 2019	Smart meter (SM)	Communication media between the UC, SM and customers, intrusion of customers, assessing SM through web applications, Customers' interference with the SM	Compromised confidentiality, Impersonation of the UC, malicious code sending to SMs, false data injection	SM shut down; Denial of service (DOS), data theft, faulty SM	Identity authentication means such as Hash Message Authentication Code-(HMAC), Physically Unclonable functions (PUF)
2020, 2011	Network Internet Protocol (IP), bypassing authentication protocols	Use of IP for data transfers	IP Spoofing, teardrop attack, compromised data integrity, data theft	Data and services theft, DOS, data modification, data fabrication, etc.	Key management system (encryption and decryption)
2019	Firmware	Firmware manipulations	False data injection (FDI) attacks, compromised integrity	Data and services theft, DOS, data modification, data fabrication, etc.	Key management system (encryption and decryption)

via the same route. (That is, from utility to the gateway, to the base station, and finally back to the customers' smart meter where it's easily received via the internet portal). The encryption was described to take place at the smart meter and the destination identity (for authentication) was included with the encrypted message before transmission.

The NS-2 environment was used for the simulation and the network area was chosen based on the available nodes in the network such that there should be no nodal overlapping in the network. The standard of measurement was the energy consumption and throughput values, dropped packets, and its delivery ratio which were found to be better when compared with previous similar schemes. The paper further emphasized the importance of securing AMI communication networks from attacks and disturbances. This was described as any launched attack on the AMI network altering the data in transmission which consequently gave wrong predictions from the utility centers' accounts for huge financial loss and can also lead to power outages with debilitating impacts.

Still on the AMI network security, [68] studied the use of multiple layered deep learning algorithms in Intrusion Detection System (IDS) together with hierarchical Support Vector Machine (SVM) algorithms, organized in a ranked pattern to accurately detect attacks in AMI components' communication network. The study buttressed the use of machine learning-based Intrusion Detection System (ML-based IDS) as one of the most used techniques in AMI attack detection in preference to ordinary IDS. This IDS attack detection technique was said to be carried out by analyzing the AMI network traffic. However, the proposed system from this study was found better when compared with a simple deep learning algorithm and SVM algorithms using the standard IMPACT- Intrusion Detection Evaluation dataset (that is, the CICIDS 2017 dataset). This is because the proposed system was found to regularly get updated with current data attacks which consequently gave a better speed for the detection ratio. The proposed system was simulated using Python 3 on a 4-gigabyte (GB) random access memory (RAM) and core i3 processor type.

In addition, the efficiency of cryptographic techniques in securing AMI networks was elaborated on [69]. This was said to largely depend on how secure the key in use is and the method should be scalable to accommodate large AMI network. All this led this study to propose identity-based cryptography for key generation, key updating, and lightweight key delivery technique with multicasting feature that involved encryption and authentication of the delivered keys and physically unclonable function (PUF) for the hardware part of AMI to avoid key compromise at that stage. According to the study, these processes were validated on a network simulator; and a key delivery delay and network traffic reduction up to 80% and 27% respectively were recorded.

STM32F2171GH microcontroller which was based on the Advanced Reduced Instruction Set Computer (RISC) Machine (ARM) cortex M3 architecture was used in mimicking smart meters due to its low power solution, minimized cost, the cryptographic hash processors and random number generators it possesses.

Also on the cryptographic solution to AMI security, Ghosal and Conti [12] surveyed the key management system (KMS) as a method of securing AMI. The paper identified the use of wireless communication as a major source of security problems in AMI and the security issues spanning from the consumers to the producers. According to this survey, attacks can be launched via false signal transmission to smart meters or even via studying customers' consumption patterns to strategize new attacks. Considering these envisaged attacks, the paper recommended the CIA Triad security requirement for AMI, which employs cryptographic measures; specifically, the KMS.

KMS was described as a system made up of a key organizational framework, key generation, and distribution alongside some storage policies. The traditional key management system which uses a single key was noted for its efficiency but least security; as obscurity is not a reliable security technique. In addition, three (3) KMS were identified for security, efficiency, scalability, and versatility. These were versatile and scalable KMS for AMI large scale (VerSAMI), VerSAMI +, and Batch-VerSAMI as improved versions for reduced computational head and speed.

Furthermore, KMS techniques in AMI were classified into 3; namely: key graph technique (the easiest, most efficient, and commonly used technique. It includes the multi-group key graph and tree key graph), authentication-based technique (such as the identity-based cryptography and two-level encryption), PUF-based technique (such as the broadcast group key management and hash chain), and the hybrid technique (such as the ID-based encryption and Advanced Encryption Standard (AES)).

Furthermore, Dhanesh Menon et al. [70] focussed on utilizing the microcontroller present in smart meters which calculates the power output and tariff rates. These data get stored via communication networks and are monitored by some artificial neural network (ANN) protocols to prevent any type of intrusion or attack targeted at it. In case of any alerted issue from the ANN, the concerned substation will trip off the relay(s) involved to stop further penetration of the attack. This was termed an ANN Protocol for blocking the AMI communication network (Table 4).

Past work done on AMI system security

AMI system, despite its notable advantages of accurate energy billings, easy tracking of power consumption rate, access to cheaper tariffs, easy-to-understand, assisting in reducing individuals' carbon footprint, etc., its vulnerability to several cyber-physical attacks remains a major challenge with different studies carried out primarily to solve this challenge. Some of these are discussed below.

Ur-Rehman et al. [9] started by differentiating between smart meters and smart metering systems. Smart meters were described to be devices with digital displays that are installed at a consumer's premises to measure and display the consumed power/commodity. Whereas, smart metering (also known as AMI) was described as an infrastructure made up of smart meters, communication networks, and other essential components for load profiles, load scheduling and remote read-out, billing and accounting, bi-directional communication, and other core functionalities. The study further identified the following security concerns in AMI. These include (a) the attacker models with different threats such as eavesdroppers, marketing agencies, customers' manipulations, active and novice attackers/mere crackers (b) the security attacks such as denial of service (DOS), packet injection, malware injection, remote connect/disconnect, firmware manipulations and MiTM attacks.

Countermeasures to the AMI security challenge were given as encrypted communications, integrity protection, authentication verification (such as digital signatures), IDS, and a gateway-based approach. The paper concluded with a proposed

Table 4 Tabular representation of the pros and cons of some AMI network security techniques

AMI network security technique	Pros	Cons	Remarks/ recommendation
CBSS scheme	Significantly minimized energy consumption and authenticates the network	It's a non-flexible scheme, only developed for the AMI communication network	More functionalities in addition to the authentication and reduced energy consumption can be worked upon
A model of multiple layered deep learning Intrusion Detection System (IDS) in conjunction with hierarchical Support Vector Machine (SVM) algorithms	The system gets regularly updated with current datasets for a better detection ratio.	- The SVM classifier is memory and time-consuming when in use for larger datasets. - SVM algorithm complexity also gets increased with an increase in the inputs' attributes - A general negative feature of IDS includes an alert of false positives/ attack detection which the study did not address.	False alarms from IDS can be worked upon
Identity-based cryptography framework with PUF	Relatively reduced latency and computational overhead	- PUF can be denatured under extreme temperature. This weakens the security strength of the proposed framework - Cryptography frameworks can be hacked via quantum computing.	The security strength can be improved
ANN protocol for blocking AMI communication network	High speed of attack detection	Higher occurrence of false detections/alarm	The protocol can be improved or hybridized for better accuracy.

security-by-design approach (SDA) as a countermeasure for the AMI security challenge. The SDA involves methods of introducing security into the AMI system by design rather than adding on when security breaches are already known. This implies that the AMI building software and hardware will be built in accordance to security analysis, design, secure implementations, and testing which is in parallel to the analysis, design, implementation, and testing of other components in the system.

Another technique for securing an AMI system is designing it in a secured Scalability, Control, and Isolation on Next-Generation Networks (SCION). This was found to give a better resilient system against possible attacks without decreasing its performance as studied [71]. The study emphasized the fact that the AMI system largely depends on the international network (internet) as a major means for transferring its data. Hence, AMI systems become vulnerable to the possible attacks on the internet.

However, SCION is known for its strong resiliency against failure recovery, MiTM, DDOS attacks, and Border Gateway Protocol (BGP) hijacking (a situation in which attackers maliciously re-route internet traffic to suit the attack purpose). In addition, SCION has dynamically re-creatable keys (DRKey) which gives an advantage of quicker and more secured authentication means. All these features secure the AMI system without compromising its performance relatively.

Furthermore, in securing AMI systems, Prabhakar et al. [72] proposed a precise and accurate Median Absolute Deviation (MAD) model for anomaly detection in AMI. The MAD model was trained with test datasets before introducing the true datasets in arriving at the final figures. It was, however, noted in the study that anomaly-based IDS can detect the least change in the parameters in use, which the signature-based IDS do not. They only identify/detect known attacks.

Ian Levy [73] discussed the importance of considering AMI system security as an integration of the security of all its components since considering AMI's single component in isolation will likely give incorrect outputs. The study further enumerated the sections constituting the AMI system to be the smart meter, MDMS, and several communication networks with their service providers.

Securing the smart meter was recommended to be through a cryptography algorithm — keyed hashed-based message authentication codes (HMAC) where each meter and each meter's message has unique authentication codes and the messages are encrypted. The smart metering key infrastructure, elliptic curve Diffie-Hellman, and ECDSA keys were other means of securing transmitting messages in the AMI system to avoid the system/entire smart grid collapsing, though with limitations as earlier mentioned in Table 1.

Table 5 gives a summary of AMI vulnerabilities, the consequences/implications of these vulnerabilities, existing solutions to them, and some specific case studies.

AMI overview and components

Advanced metering infrastructure (AMI), also known as smart metering is an important component of the smart grid that is usually responsible for the smartness of the grid [12]. It is an interphase between the user and the utility domains [11]. AMI exhibits a complex network formation process and comprises several cyber-physical components that are linked via different communication media and security measures [10] (Table 6).

The structure/major components of AMI

Figure 2 shows the AMI framework which comprises the following elements; 2-way communication channels, smart meters, the meter data management system (MDMS), and several types of networks (body area network (BAN), home area network (HAN), etc.).

The smart meters are automated meters with additional functionalities of exchanging pricing information and direct load control commands for energy optimization and active demand response [3]. They consist of metering circuitry that collects and measures energy consumption (data) and a communication interface for handling communications with other nodes. The MDMS carries, verifies, processes and stores collected data before making it available for billing and analysis. Also, connecting the smart meters to the utility is done via technologies and network interface (the demand response management system (DRMS)) which control the demands and allow users to control their level and pattern of electricity usage. In general, the AMI uses both wired and wireless links (power line and cellular communications) along with several internet protocols (IP) for its communication processes, and due to their insecure nature, AMI networks and data are prone to various security threats and attacks [87].

Below is a summary of the communication media and protocol in AMI as described by Mattioli, R and Moulinos [88].

Table 5 Tabular representation of AMI system vulnerabilities, its implications, existing countermeasures, and specific case studies

AMI system vulnerabilities	Past security breaches in AMI	Existing countermeasures to the vulnerability type	Implication/consequences of the Vulnerability Type
Authentication and access control weaknesses [74, 75]	- In 2018, Puerto Rico's utility company, PREPA, suffered a cyber-attack on its AMI system. The breach highlighted vulnerabilities in the utility's infrastructure and the need for enhanced cybersecurity measures in AMI systems [76]	Strong authentication techniques such as public key infrastructure (PKI) cryptographic protocols and signatures, and two-factor authentication [77, 78]	Weak authentication and access control techniques can allow unauthorized access to the AMI system, false data injection (FDI) attacks, and manipulations of the meter data. This consequently compromises the integrity and confidentiality of the smart metering data [79].
AMI software and communication protocol vulnerabilities [80]	- In 2016, the Burlington Electric Department in Vermont detected Russian malware on one of its computers connected to the grid's AMI system. While the malware did not compromise the grid's operations, it underscored the vulnerability of utility systems to cyber threats and the need for continuous monitoring and robust security protocols	- Implementing secure communication protocols with efficient encryption and authentication techniques [81] - Regularly updating firmware and software to patch known vulnerabilities, and - Segmentation of the network to isolate critical components from potential threats	AMI communication protocols (such as the Wi-Fi and cellular network) are prone to attacks such as eavesdropping, replay, and MiTM attacks. These attacks consequently breach the confidentiality of the AMI data
Artificial intelligence (AI)-power jamming attack	Malicious actors injected false data into the training datasets of AI models used for demand forecasting in AMI systems. By tampering with historical consumption data, the attacker was able to manipulate future predictions, thereby disrupting load balancing and grid operations.	- Implementing intrusion detection systems to detect and mitigate abnormal network traffic patterns	This involves adversaries employing reinforcement learning to dynamically adjust jamming patterns to disrupt communication between smart meters and the central management system. Thereby, causing delay and or unavailability of service [82]
Adversarial attacks on smart meters' data		- Implementing anomaly detection algorithms to flag unusual readings (regardless of how small the deviation is), for manual inspection and verification [83]. - Employing encryption and digital signatures to ensure data integrity [84].	This type of vulnerability can involve adversaries using generative adversarial networks (GANs) to manipulate meter readings; thereby compromising data confidentiality, authentication, and integrity. This can cause financial losses for utilities when energy consumption is under-reported and also disruptions of the grid operations

Table 5 (continued)

AMI system vulnerabilities	Past security breaches in AMI	Existing countermeasures to the vulnerability type	Implication/consequences of the Vulnerability Type
Denial of service (DOS) attacks [15]	- In 2015 and 2016, Ukraine experienced several cyber-attacks on its power grid, impacting AMI systems and leading to widespread power outages. The attacks involved sophisticated malware that disrupted communication systems and control functions, emphasizing the importance of securing critical infrastructure like an AMI system.	- Implementing network traffic monitoring and filtering tools - Deploying firewalls and intrusion prevention and detection systems (IPS and IDS) - Maintaining redundant infrastructure to mitigate the impact of DoS attacks [83]	These target the availability of the AMI system, such as flooding the network with excessive traffic or overwhelming system resources
Inadequate encryption of data transmitted between smart meters and the central AMI system [67].	Smart meters' data manipulations in Ghana which led to wrong/falsified billings that consequently led to a huge loss for the utility company [85]	- Usage of strong encryption algorithms; especially those resistant to both classical and quantum attacks (e.g., AES, lattice-based cryptography, code-based cryptography, etc.) to protect data in transit and at rest [86] - Implementing secure key management practices, and regularly updating encryption protocols to address emerging threats.	Weak/poor data encryption exposes sensitive information to interception, manipulation, FDI attacks, and or tampering

Table 6 Tabular representation of the pros and cons of some AMI system security techniques

AMI system security technique	Pros	Cons	Remarks/ recommendation
Security by design approach (SDA)	It's a preventive measure against attacks which saves time, cost, and resources when compared to corrective/mitigation measures that function after an attack is launched and losses are already incurred.	It increases the cost of AMI installation; thereby discouraging/delaying its deployment. - It is relatively a non-flexible security technique that incurs higher costs for Upgrading an already built system in cases of the latest inventions	Other corrective measures should be used parallel to SDA.
Scalability, Control and Isolation on Next-Generation Networks (SCION) platform for AMI system	Gives strong resiliency against failure recovery and some other major AMI attacks	- Its implementation usually requires additional overhead to the whole system which introduces a longer time for the data reading process - Some components of AMI are not internet-dependent. Hence, an anon-internet security loophole	Can be hybridized with other techniques for an all-round security

Wired: Broadband over power lines power-line communication (BPL PLC), distribution line carrier PLC (DLC PLC), fiber, twisted pair, plesiochronous digital hierarchy (PDH), Synchronous Optical Network/Synchronous digital hierarchy (SONET/SDH), Plain Old Telephone Service (POTS), PoweRline Intelligent Metering Evolution PLC (PRIME PLC), Meters & More (PLC), American National Standards Institute (ANSI) C12.18, ANSI C12.21.

Wireless: radio frequency, microwave, cellular, long-term evolution (LTE), general packet radio services (GPRS), universal mobile telecommunications system (UMTS), institute of Electrical Electronics Engineers (IEEE) 802.16 worldwide interoperability for microwave access (WiMAX).

Medium independent: Transmission Control Protocol/Internet Protocol (TCP/IP) suite, ANSI C12.22.

AMI architecture and its communication protocols

As aforementioned and shown in Fig. 3, AMI interconnects the users/smart meters and the utilities (utility server and MDMS). This consequently leads to its use of different protocols; depending on preference and suitability with the communication network. These protocols can be wired or wireless. For example, a power-line communication (PLC)-based protocol; as seen in PRIME, which combines with device language message specification/Companion specification for Energy metering (DLMS/COSEM), the long-term evolution (LTE) 4G cellular-based protocol, or the ZigBee which combines with other technologies such as the global system for mobile communication (GSM) [89].

The DLMS/COSEM protocol is the usual protocol for AMI implementation and it commonly works with PRIME-which is a PLC-based protocol. The DLMS/COSEM works in a client–server setting where signals/information such as critical alarms are

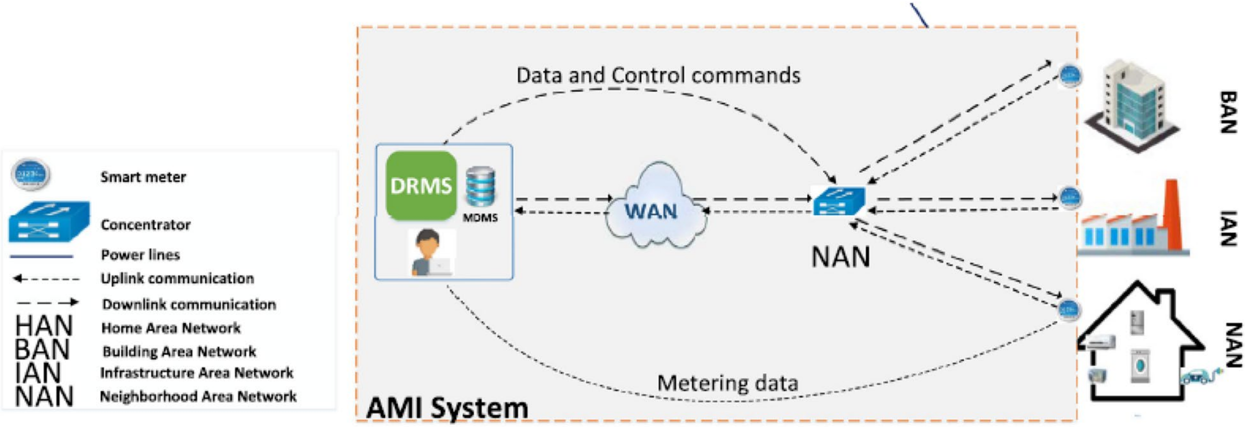

Fig. 2 The structure of AMI; its components and networks [87]

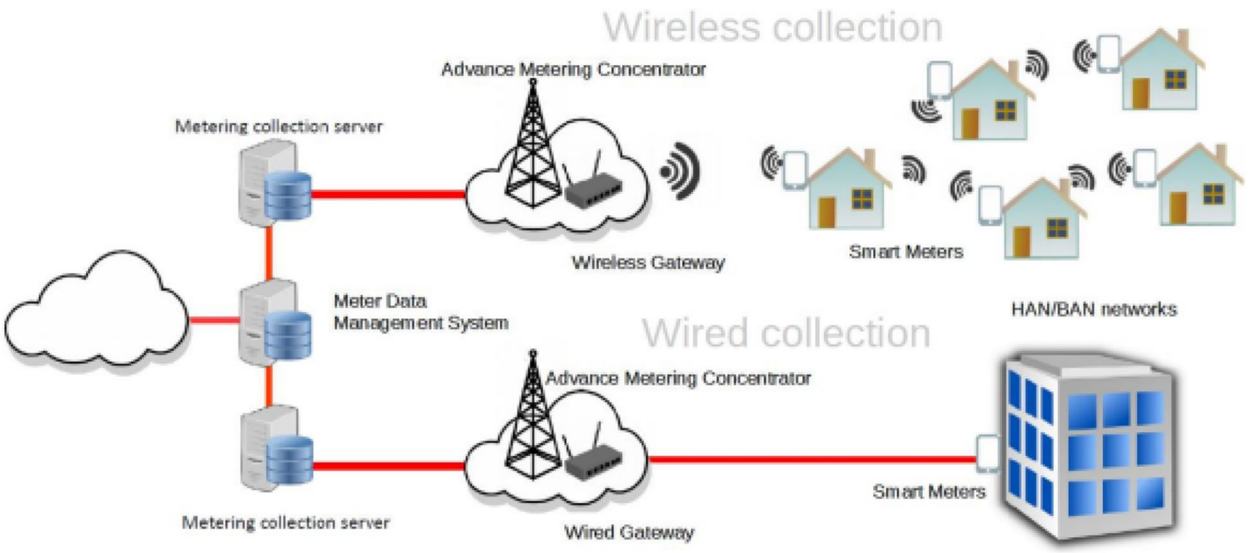

Fig. 3 AMI architecture [88]

directly sent to the client. Here, the end devices are the client and the smart meters work as the server. Also, this protocol is characterized by features that support some levels of security. Examples are its message protection feature (which supports cryptographic protection for maintaining the confidentiality and integrity of any sent or received information) and its role-based authentication feature [58, 88].

The long-term evolution (LTE) protocol is a 4G cellular communication protocol that gives good and secure packet data switching, high capacity, cost-effectiveness, and low latency when used in the AMI system. Its low-latency unique feature makes it more advantageous than other communication protocols when implemented in the AMI system, where reliable security measure is a trade-off for latency [73, 90, 91].

The ZigBee protocol is specifically designed and mostly used in low-power devices/applications (devices with data rates of 250kbps or less). Though technically possible for ZigBee to be used through a PLC as seen in AMI, it is usually used through a physical-MAC layer of the IEEE 802.15 standard. It also possesses some communication security features; which is an advantage when used in AMI [88].

The PLC-based protocol exists as either narrowband or broadband PLC. The broadband is characterized with a relatively high frequency within the range of 2–30 MHz, a relatively high data rate but a disadvantage of relatively high cost. However, with attenuation being proportional to frequency (which is high), there's a need for repeaters which introduces additional cost and also latency to the system. Hence, in ensuring maximum reduction of latency in AMI operations, the broadband PLC is not advisable [31].

The narrowband PLC on the other hand is characterized by lower carrier frequencies which annuls the need for repeaters. Examples of this type of PLC are PRIME and G_3-PLC. The PRIME Protocol is a public, non-proprietary narrowband power-line communication protocol (NB-PLC) that is mostly used in AMI for fulfilling the present and future needs of the smart grid. PRIME has been implemented in over 20 million smart meters across fifteen countries [92] and the G_3-PLC implemented in more than 80 million devices in over 30 countries [93].

PRIME protocol is based on international standard ITU G.9904 and it's made up of layers such as the physical layer (which uses Orthogonal Frequency Division Multiplexing-OFDM modulation to receive and transmit data packets between nodes), convergence layer (which groups network traffic to their corresponding MAC layer), Media Access Control (MAC) Layer (which also gives access, bandwidth, topology resolution and connection management) and other layers as shown in Fig. 4 [94].

In addition to the discussed communication protocols for AMI, there also exists the Open Smart Grid Protocol (also known as GS OSG 001) and the Meters and More (M & M) Protocol, both with different features. The former defines different specifications that control the application of smart grid components like the AMI over the standard communication network. It gives reliable and efficient delivery methods for data transfer/control to smart meters. It also aids load control modules, gateways, and solar panels. The latter protocol is a centralized system that controls the network metering process. It improves the robustness and agility of the communication network in use and also allows automatic network configuration, transmission management, and ease in the usage of the 128-bit AES encryption method [31, 34, 35].

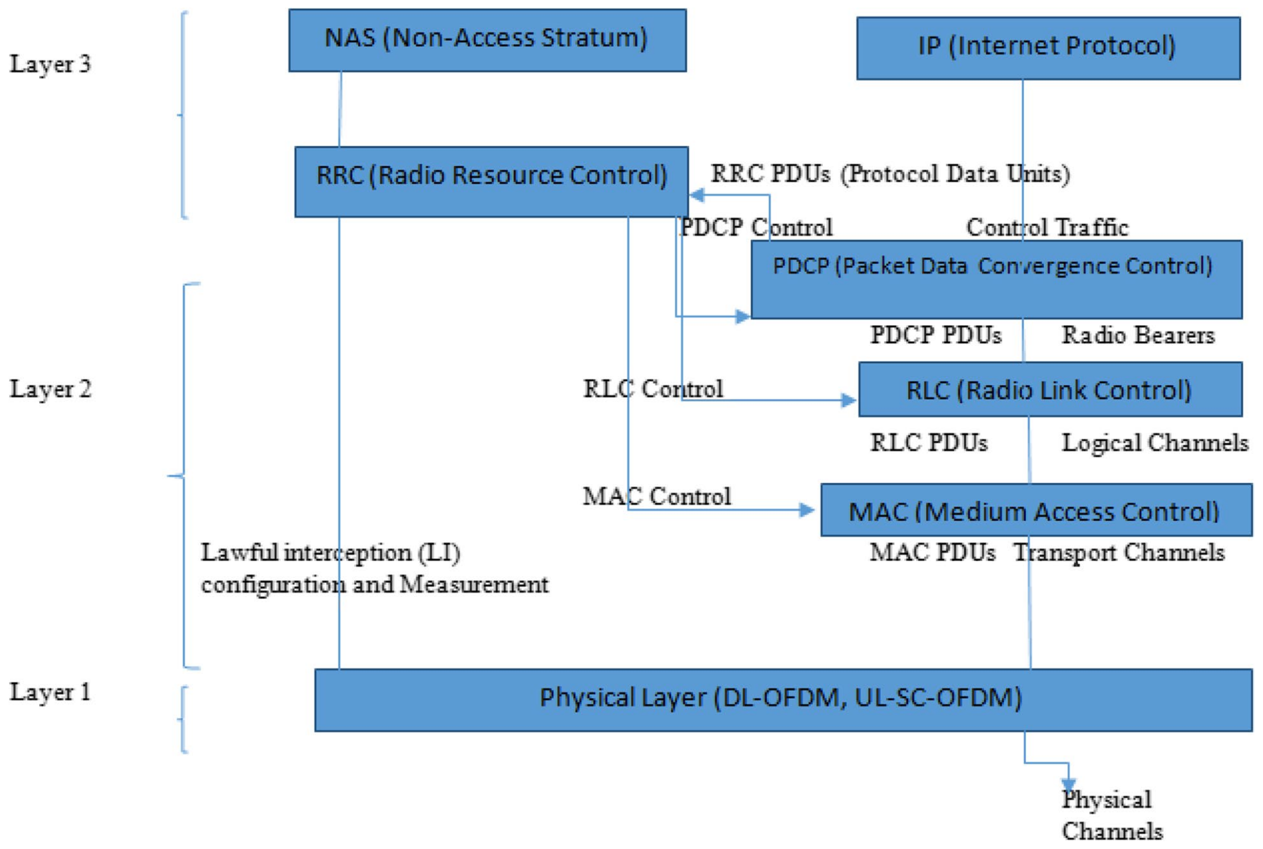

Fig. 4 The PRIME Protocol Layers [94]

A tabular summary of some of the vulnerabilities of AMI protocols and suggested countermeasures are given in Table 7.

Countermeasure techniques

The countermeasure techniques for AMI cyber-physical threats and attacks can be broadly classified as either cryptographic or non-cryptographic techniques. The non-cryptographic techniques exist as battery-based load hiding or physically unclonable function (PUF). However, the battery-based load hiding has major disadvantages of relatively high cost and shorter lifespan which discourage its usage in securing AMI [100, 101].

However, the PUF, despite its high-security function under relatively standard conditions, easily gets denatured under extreme weather conditions/temperature; thereby, weakening its security strength [27]. This leaves the cryptographic technique as the deplorable method of securing AMI.

Table 7 Tabular representation of AMI protocol vulnerabilities, its implications/consequences, and existing countermeasures

S/N	AMI protocol type	AMI protocol vulnerability and its consequences	Existing countermeasures to the vulnerability type
1	Zigbee	Zigbee networks are susceptible to eavesdropping, replay attacks, communication interruption, and unauthorized access due to the weak encryption in their default configurations. This consequently compromises the confidentiality, integrit,y and availability of the transmitted data and services in general [80]	Implementing strong encryption algorithms (e.g., ECC and AES-128) - Usage of unique network keys - Regularly updating firmware to patch known vulnerabilities. - Segmenting Zigbee networks to limit the impact of potential compromises [95]
2	Wireless fidelity (Wi-Fi)	Vulnerable to attacks such as the service set identifier (SSID) forgery, evil twin attack, etc. which compromises the confidentiality and integrity of the transmitted data and or signals [96].	- Implementing Wi-Fi Protected Access (WPA2 or WPA3) with strong encryption and authentication. - Enabling intrusion detection and prevention systems (IDPS). - Regularly monitoring network traffic for suspicious activity. - Enforcing strong password policies and usage of secure Wi-Fi configurations [97]
3	Power-line communication (PLC)	PLC-based AMI systems can be susceptible to signal interception, relay attacks, and signal injection attacks if the power-line communication medium is not adequately secured. Consequently,resulting into signal manipulations [98]	- Implementing efficient encryption and authentication protocols designed for PLC communication - Usage of signal filtering and error-checking mechanisms to detect and prevent signal manipulations - Conducting regular security assessments of PLC infrastructure to identify and mitigate vulnerabilities [99]
4	Cellular network (LTE, 3G,4G, 5G)	Cellular networks used for AMI communication may be susceptible to interception of data, SIM card cloning, and denial-of-service (DoS) attacks, targeting network infrastructure. Thereby, energy losses from data manipulations, unavailability of services, etc. [15]	- Implementing efficient encryption and authentication mechanisms provided by the cellular network operator - Usage of virtual private networks (VPNs) to secure data transmission - Deploying firewalls and intrusion detection systems (IDS) to monitor and protect network traffic [15]

The cryptographic technique involves the use of public/asymmetric key, private/symmetric key, hashing, homomorphic encryption, and hybrid schemes involving the combinations of any of these techniques to achieve the security objectives of confidentiality, integrity, authentication, availability, and non-repudiation of information in AMI [5].

In achieving these security objectives, different cryptography methods work better for different cryptography processes. For example, Advanced Encryption Standard (AES), and Data Encryption Standard (DES). Elgamal scheme or Rivest-Shamir Adleman (RSA) algorithm is a suitable technique for achieving secured data encryption with high complexity. However, the smart grid being an Internet-of-Things (IoT) device with limited storage capacity, limits the cryptography type applicable to securing it since most cryptographic functions involve large computations. Hence, lightweight cryptography (commonly known as the elliptic curve cryptography (ECC)) modifications have been explored to suit AMI security.

Vahedi et al. [47] and Sunuwar and Samal [102] proposed a privacy-preserving scheme using ECC based on the Elgamal cryptosystem with relatively: efficient computation cost for the users, lesser computation, communication overheads when compared to other schemes, and security in the absence of quantum computing.

In summary, listed below are the general measures and recommendations for mitigating these threats and attacks.

1. Employee training: This involves conducting comprehensive training programs for employees, emphasizing security best practices to mitigate the risk of social engineering attacks and other security breaches.
2. Physical security measures for SMs: Designing smart meters with effective physical security features to thwart tampering attempts
3. Authentication: Implementing stringent authentication measures such as signature schemes for smart meters to deter unauthorized access. However, this alone does not maintain the meter's data integrity and confidentiality as achieved by the encryption method.
4. Software updates: Regularly and timely provision of software updates is crucial to address vulnerabilities and enhance the overall security of the AMI system.
5. Encryption: It is important to incorporate robust encryption in the smart meters to safeguard the energy data both during transit and when stored. The cryptography encryption method, specifically the key management system (KMS) as mentioned earlier, has been found efficient for AMI [103].

Open issues/future research

As technology evolves rapidly, securing AMI becomes a challenge; especially with the advent of quantum computing. This is because quantum computers can successfully breach existing renowned AMI cryptographic security [104]. Hence, hybridizations and modifications of existing quantum-resistant security schemes such as quantum encryption, and post-quantum cryptography (PQC) with lightweight techniques of lesser computations can be explored in future research for efficiently securing AMI.

In addition, the implementation of advanced blockchain technology and machine learning techniques can also be investigated for accurate detection and mitigation of threats and attacks in AMI. Below are some of these existing advanced countermeasures techniques for AMI security which are still open to further research.

Implementing lattice-based cryptography which is a type of PQC scheme, for AMI security against quantum and classical attacks, was investigated and found compatible. Its variant schemes with lesser delay and lesser computational complexities are encouraged to be developed [86, 104, 105]. Artificial intelligence methods/machine learning techniques were also explored for AMI security [106, 107]. The techniques were found to be relatively accurate with a high detection rate. However, the advanced blockchain technique was also successfully implemented for smart metering security against classical and quantum attacks; though with limitations of high latency/delay [28, 108, 109]. All these advanced techniques for securing AMI are open to improvements for future work.

Conclusions

This paper gives a comprehensive review of the privacy and security of AMI data and networks. This comprises the existing related review papers for AMI data and network vulnerabilities and their proposed countermeasure techniques with their strengths, and limitations. Based on these reviews, the key management cryptographic technique emerged as the most deployed promising solution to AMI vulnerabilities among others.

The uniqueness and contributions of this review paper lie in its identification of the existing state-of-the-art AMI security techniques. These are the PUF, AI, PQC, QE, blockchain techniques, etc. with their pros and cons, specific vulnerabilities of the AMI system and its protocols, and the impacts of these vulnerabilities, with their corresponding countermeasures, and possible future research in this area.

Some of the identified vulnerabilities of the AMI system and protocols include weak authentication and encryption techniques, adversarial attacks on smart meters' data, and AI-power jamming attacks. While some of the mentioned impacts of these vulnerabilities include the FDI, MiTM attacks, eavesdropping, and delays/obstruction in data transmissions.

As part of the stated contribution of this review paper, relatively improving advanced countermeasure techniques such as the PQC, and advanced blockchain techniques to reduce their accompanying large delays/execution time, and or hybridizing them with AI techniques for improved efficient security can be explored for future work.

Abbreviations

SG	Smart grid
AMI	Advanced metering infrastructure
ICT	Information communication technology
ECC	Elliptic curve cryptography
IoT	Internet of Things
AES	Advanced Encryption Standard
DES	Data Encryption Standard
RSA	Rivest-Shamir Adleman
CIA/AIC	Confidentiality, Integrity, Availability/Availability, Integrity, Confidentiality
USA	United States of America
MiTM	Man-in-the-middle
KMS	Key management system/key management scheme
SMS	Short message service
IDS	Intrusion detection system
DOS	Denial of service
DDOS	Distributed denial of service

MDMS	Meter data management system
FDI	False data injection
ID	Identity
UN	United Nations
ECBDA	Elliptic Curve-Based Data Aggregation
DP	Differential privacy
GAP	Generative adversarial privacy
DNN	Deep neural network
UK	United Kingdom
HAN	Home area network
NAN	Neighborhood area network
WAN	Wide area network
FAN	Field area network
IAN	Infrastructure area network
SM(s)	Smart meter(s)
UC	Utility center
DC	Data center
HMAC	Hash Message Authentication Code
PUF	Physically unclonable function
IP	Internet Protocol
CBSS	Concealed-based security scheme
SVM	Support Vector Machine
ML	Machine learning
ARM	Advanced RISC Machine
RISC	Reduced Instruction Set Computer
VerSAMI	Versatile and scalable key management scheme for AMI
ANN	Artificial neural network
SDA	Security by design
SCION	Scalability, Control and Isolation On next generation Networks
BGP	Border Gateway Protocol
DRKey	Dynamically Recreatable Key
MAD	Median absolute derivation
SDA	Security by design approach
DRMS	Demand response management system
PRIME	PoweRline Intelligent Metering Evolution
PLC	Power-line communication
DLMS/COSEM	Device Language Message Specification/Companion Specification for Energy Metering
NAS	Non-access stratum
RRC	Radio Resource Control
RLC	Radio Link Control
MAC	Medium Access Control
PDCP	Packet Data Convergence Control
PDU	Protocol Data Unit
OSG	Open Smart Grid
UL-SC-OFDM	Uplink-Single Carrier-Orthogonal Frequency Division Multiplexing
DL-OFDM	Downlink-Orthogonal Frequency Division Multiplexing
WIMAX	Worldwide Interoperability for Microwave Access
M & M	Meters & More
NS-2	Network Simulator Version 2
GPRS	General Packet Radio Services
UMTS	Universal Mobile Telecommunications System
IEEE	Institute of Electrical Electronics Engineers
BPL	Broadband over Power Lines
DLC	Distribution Line Carrier
PDH	Plesiochronous Digital Hierarchy
SONET/SDH	Synchronous Optical Network/Synchronous Digital Hierarchy
POTS	Plain Old Telephone Service
ANSI	American National Standards Institute
TCP/IP	Transmission Control Protocol/Internet Protocol
LI	Lawful interception

Acknowledgements

The authors of this review paper would like to acknowledge the KNUST Engineering Education Project (KEEP), Kumasi-Ghana, for their financial assistance towards the research study that produced this manuscript and their commitment to advancing engineering knowledge.

Authors' contributions

The initial draft of this manuscript was written by POA and it was sequentially reviewed by KO-BOA and EAF who informed POA of the necessary changes to effect in the manuscript. The three (3) authors made substantial contributions to this manuscript and read and approved the final manuscript.

Funding

The entire research study that produced this review manuscript at the initial stage of the research is funded by the KNUST Engineering Education Project (KEEP), Kumasi-Ghana.

Availability of data and materials

Not applicable.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 14 July 2023 Accepted: 30 March 2024
Published online: 12 April 2024

References

1. Yadav SA, Kumar SR, Sharma S, Singh A (2016) "A review of possibilities and solutions of cyber attacks in smart grids", 2016 1st Int. Conf Innov Challenges Cyber Secur ICICCS 2016:60–63. https://doi.org/10.1109/ICICCS.2016.7542359
2. Kebotogetse O, Samikannu R (2021) Review of key management techniques for advanced metering infrastructure. 17(8). https://doi.org/10.1177/15501477211041541
3. Asghar MR, Dán G, Miorandi D, Chlamtac I (2017) Smart meter data privacy: A survey. IEEE Commun Surv Tutorials 19(4):2820–2835. https://doi.org/10.1109/COMST.2017.2720195
4. Kayalvizhy V, Banumathi A (2021) A Survey on Cyber Security Attacks and Countermeasures in Smart Grid Metering Network. Proc. - 5th Int. Conf. Comput. Methodol. Commun. ICCM; pp. 160–165. https://doi.org/10.1109/ICCMC51019.2021.9418303
5. "Understanding Cryptography, A Textbook for Students and Practitioners - with a Foreword by Bart Preneel." https://www.crypto-textbook.com/index.php. Accessed 10 May 2022
6. Fanlin M, Wei Y (2020) Summary of Research on Security and Privacy of Smart Grid. Proc. - 2020 Int. Conf. Comput. Commun. Netw. Secur. CCNS; pp. 39–42. https://doi.org/10.1109/CCNS50731.2020.00017.
7. Alfassa SM, Nagasundari S, Honnavalli PB (2021) "Invasion Analysis of Smart Meter in AMI System", 2021 IEEE Mysore Sub Sect. Int Conf MysuruCon 2021:831–836. https://doi.org/10.1109/MYSURUCON52639.2021.9641595
8. Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A (2019) Smart grid metering networks: a survey on security, privacy and open research issues. IEEE Commun Surv Tutorials 21(3):2886–2927. https://doi.org/10.1109/COMST.2019.2899354
9. Ur-Rehman O, Zivic N, Ruland C (2015) Security issues in smart metering systems. Int. Conf. Smart Energy Grid Eng. SEGE. https://doi.org/10.1109/SEGE.2015.7324615
10. Anzalchi A, Sarwat A (2015) A survey on security assessment of metering infrastructure in Smart Grid systems. Conf. Proc. - IEEE SOUTHEASTCON. vol. 2015. https://doi.org/10.1109/SECON.2015.7132989
11. Shokry M, Awad AI, Abd-Ellah MK, Khalaf AAM (2022) Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. Futur Gener Comput Syst 136:358–377. https://doi.org/10.1016/J.FUTURE.2022.06.013
12. Ghosal A, Conti M (2019) Key Management systems for smart grid advanced metering infrastructure: a survey. IEEE Commun Surv Tutorials 21(3):2831–2848. https://doi.org/10.1109/COMST.2019.2907650
13. Desai S, Alhadad R, Chilamkurti N, Mahmood A (2019) A survey of privacy preserving schemes in IoE enabled Smart Grid Advanced Metering Infrastructure. Cluster Comput 22(1):43–69. https://doi.org/10.1007/S10586-018-2820-9
14. El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H (2018) Cyber-security in smart grid: Survey and challenges. Comput Electr Eng 67:469–482. https://doi.org/10.1016/J.COMPELECENG.2018.01.015
15. Pedramnia K, Rahmani M (2018) Survey of DoS Attacks on LTE infrastructure used in AMI System and Countermeasures. Proc. - 2018 Smart Grid Conf. SGC. https://doi.org/10.1109/SGC.2018.8777832
16. Hansen A, Staggs J, Shenoi S (2017) Security analysis of an advanced metering infrastructure. Int J Crit Infrastruct Prot 18:3–19. https://doi.org/10.1016/J.IJCIP.2017.03.004
17. Tan S, De D, Song WZ, Yang J, Das SK (2017) Survey of security advances in smart grid: a data driven approach. IEEE Commun Surv Tutorials 19(1):397–422. https://doi.org/10.1109/COMST.2016.2616442
18. Tong W, Lu L, Li Z, Lin J, Jin X (2016) A survey on intrusion detection system for advanced metering infrastructure. Proc. - 2016 6th Int. Conf. Instrum. Meas. Comput. Commun. Control. IMCCC. pp. 33–37. https://doi.org/10.1109/IMCCC.2016.193
19. Jokar P, Arianpoo N, Leung VCM (2016) A survey on security issues in smart grids. Secur Commun Networks 9(3):262–273. https://doi.org/10.1002/SEC.559
20. Saxena N, Choi BJ (2015) State of the art authentication, access control, and secure integration in smart grid. Energies 8(10):11883–11915. https://doi.org/10.3390/EN81011883
21. Chris Foreman J, Gurugubelli D (2015) Identifying the cyber attack surface of the advanced metering infrastructure. Electr J 28(1):94–103. https://doi.org/10.1016/J.TEJ.2014.12.007
22. Rashed Mohassel R, Fung A, Mohammadi F, Raahemifar K (2014) A survey on Advanced Metering Infrastructure. Int J Electr Power Energy Syst 63:473–484. https://doi.org/10.1016/J.IJEPES.2014.06.025

23. Ancillotti E, Bruno R, Conti M (2013) The role of communication systems in smart grids: Architectures, technical solutions and research challenges. Comput Commun 36(17–18):1665–1697. https://doi.org/10.1016/J.COMCOM.2013.09.004
24. Na L, Xiaohui X, Xiaoqin M, Xiangfu M, Peisen Y (2021) Fake Data Injection Attack Detection in AMI System Using a Hybrid Method. Proc. - 2021 IEEE Sustain. Power Energy Conf. Energy Transit. Carbon Neutrality. iSPEC; pp. 2371–2376. https://doi.org/10.1109/ISPEC53008.2021.9735875
25. Tyav J, Tufail S, Roy S, Parvez I, Debnath A, Sarwat A (2020) A comprehensive review on Smart Grid Data Security. Conf Proc - IEEE SOUTHEASTCON 2022:8–15. https://doi.org/10.1109/SOUTHEASTCON48659.2022.9764139
26. YCao YN, Wang Y, Ding Y, Zheng H, Guan Z, Wang H (2021) A PUF-based Lightweight Authenticated Metering Data Collection Scheme with Privacy Protection in Smart Grid. 19th IEEE Int. Symp. Parallel Distrib. Process. with Appl. 11th IEEE Int. Conf. Big Data Cloud Comput. 14th IEEE Int. Conf. Soc. Comput. Netw. 11th IEEE Int; pp. 876–883. https://doi.org/10.1109/ISPA-BDCloud-SocialCom-SustainCom52081.2021.00124
27. Anagnostopoulos NA, Arul T, Rosenstihl M, Schaller A, Gabmeyer S, Katzenbeisser S (2019) Attacking SRAM PUFs using very-low-temperature data remanence. Microprocess Microsyst 71:102864. https://doi.org/10.1016/J.MICPRO.2019.102864
28. Tian H, Jian Y, Ge X (2022) Blockchain-based AMI framework for data security and privacy protection. Sustain Energy Grids Netw 32:100807. https://doi.org/10.1016/J.SEGAN.2022.100807
29. Cao YN, Wang Y, Ding Y, Guo Z, Wu Q, Liang H (2023) Blockchain-empowered security and privacy protection technologies for smart grid. Comput. Stand. Interfaces 85(June 2022):103708. https://doi.org/10.1016/j.csi.2022.103708
30. V. V. Vineeth and S. Sophia, "Data Falsification Detection in AMI: A Secure Perspective Analysis," Artif. Intell. Renew. Energy Syst., pp. 201–209, Feb. 2022, doi: https://doi.org/10.1002/9781119761686.CH9.
31. Ogu RE, Ikerionwu CI, Ayogu II (2021) Leveraging artificial intelligence of things for anomaly detection in advanced metering infrastructures. Proc. 2020 IEEE 2nd Int. Conf. Cyberspace, CYBER Niger. pp. 16–20. https://doi.org/10.1109/CYBERNIGERIA51635.2021.9428792
32. Kong PY (2022) A review of quantum key distribution protocols in the perspective of smart grid communication security. IEEE Syst J 16(1):41–54. https://doi.org/10.1109/JSYST.2020.3024956
33. Li Y, Zhang P, Huang R (2019) Lightweight quantum encryption for secure transmission of power data in smart grid. IEEE Access 7:36285–36293. https://doi.org/10.1109/ACCESS.2019.2893056
34. Mariot L, Picek S, Yorgova R (2023) On McEliece-type cryptosystems using self-dual codes with large minimum weight. IEEE Access 11(August):43511–43519. https://doi.org/10.1109/ACCESS.2023.3271767
35. Khan AA, Kumar V, Ahmad M, Rana S (2021) LAKAF: Lightweight authentication and key agreement framework for smart grid network. J Syst Archit 116:102053. https://doi.org/10.1016/J.SYSARC.2021.102053
36. Putu Agus Eka Pratama I, Gusti Ngurah Agung Krisna Adhitya I (2022) Post Quantum Cryptography: Comparison between RSA and McEliece. 9th Int. Conf. ICT Smart Soc. Recover Together, Recover Stronger Smarter Smartization, Gov. Collab. ICISS 2022 - Proceeding. https://doi.org/10.1109/ICISS55894.2022.9915232
37. Gopstein A, Nguyen C, O'Fallon C, Hastings N, Wollman DA (2021) NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. https://doi.org/10.6028/NIST.SP.1108R4
38. Robles T, Bordel B, Alcarria R, Sánchez-de-Rivera D (2018) Blockchain technologies for private data management in AmI environments. Proceedings 2(19):1230. https://doi.org/10.3390/PROCEEDINGS2191230
39. Fathiyana RZ, Hidayat F, Rahardjo B (2020) An Integration of National Identity towards Single Identity Number with Blockchain. https://doi.org/10.4108/eai.12-10-2019.2296532
40. Khacef K, Pujolle G (2019) Secure Peer-to-Peer communication based on Blockchain. pp. 662–672
41. Yigit M, Gungor VC, Baktir S (2014) Cloud computing for smart grid applications. Comput Networks 70:312–329. https://doi.org/10.1016/J.COMNET.2014.06.007
42. Pau M et al (2018) A cloud-based smart metering infrastructure for distribution grid services and automation. Sustain Energy Grids Networks 15:14–25. https://doi.org/10.1016/J.SEGAN.2017.08.001
43. Brito A et al (2019) Secure end-to-end processing of smart metering data. J Cloud Comput 8(1):1–13. https://doi.org/10.1186/S13677-019-0141-Z/FIGURES/11
44. "Human Rights Council Twenty-third session Agenda item 3 Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* Summary". https://www.ohchr.org/en/news/2023/09/human-rights-council-continues-general-debate-promotion-and-protection-all-human
45. Lee D, Hess DJ (2021) Data privacy and residential smart meters: Comparative analysis and harmonization potential. Util Policy 70:101188. https://doi.org/10.1016/J.JUP.2021.101188
46. Jawurek M (2013) Privacy in Smart Grids. Opus4.Kobv.De. pp. 1–256. Available: http://opus4.kobv.de/opus4-fau/files/3645/Dissertation_MarekJawurek_fuer_finalen_Druck_1.0.pdf
47. Vahedi E, Bayat M, Pakravan MR, Aref MR (2017) A secure ECC-based privacy preserving data aggregation scheme for smart grids. Comput Networks 129:28–36. https://doi.org/10.1016/J.COMNET.2017.08.025
48. Gough MB, Santos SF, Alskaif T, Javadi MS, Castro R, Catalao JPS (2022) Preserving privacy of smart meter data in a smart grid environment. IEEE Trans Ind Informatics 18(1):707–718. https://doi.org/10.1109/TII.2021.3074915
49. Shateri M, Messina F, Piantanida P, Labeau F (2020) Real-Time Privacy-Preserving Data Release for Smart Meters. IEEE Trans Smart Grid 11(6):5174–5183. https://doi.org/10.1109/TSG.2020.3005634
50. Abdalzaher MS, Fouda MM, Ibrahem MI (2022) Data privacy preservation and security in smart metering systems. Energies 15(19):1–19. https://doi.org/10.3390/en15197419
51. C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," pp. 238–243, 2010, doi: https://doi.org/10.1109/smartgrid.2010.5622050.
52. "Consumer privacy concerns limit smart meter data access in GB – report."https://www.smart-energy.com/industry-sectors/smart-meters/consumer-privacy-concerns-limit-smart-meter-data-access-in-gb-report/. Accessed 16 Dec 2022
53. C. Cuijpers, "Courts, privacy and data protection in the Netherlands: European influence and trends in litigation.," Court. Priv. Data Prot. Digit. Environ., pp. 162–179, May 2017, doi: https://doi.org/10.4337/9781784718718.00016.

54. Hielscher S, Sovacool BK (2018) Contested smart and low-carbon energy futures: Media discourses of smart meters in the United Kingdom. J Clean Prod 195:978–990. https://doi.org/10.1016/J.JCLEPRO.2018.05.227
55. Buchanan K, Banks N, Preston I, Russo R (2016) The British public's perception of the UK smart metering initiative: Threats and opportunities. Energy Policy 91:87–97. https://doi.org/10.1016/J.ENPOL.2016.01.003
56. Draetta L, Tavner B (2019) De la « fronde anti-Linky » à la justification écologique du smart metering : retour sur la genèse d'un projet controversé. Lien Soc Polit 82:52–77. https://doi.org/10.7202/1061876AR
57. "The factors behind low smart meter penetration in Africa." https://www.smart-energy.com/policy-regulation/the-factors-behind-low-smart-meter-penetration-africa/ (accessed Dec. 16, 2022).
58. Ngcobo TJ, Ghayoor F. An overview of DLMS/COSEM and g3-plc for smart metering applications. Int J Smart Sens Intell Syst. 2022;15(1). https://doi.org/10.2478/IJSSIS-2022-0011
59. Tweneboah-Koduah S, Tsetse AK, Azasoo J, Endicott-Popovsky B (2018) Evaluation of cybersecurity threats on smart metering system. Adv Intell Syst Comput 558:199–207. https://doi.org/10.1007/978-3-319-54978-1_28
60. Aouini I, Ben Azzouz L, Saidane LA (2016) A secure neighborhood area network using IPsec. 2016 Int. Wirel. Commun. Mob. Comput. Conf. IWCMC. pp. 102–107. https://doi.org/10.1109/IWCMC.2016.7577041
61. He H, Yan J (2016) Cyber-physical attacks and defences in the smart grid: a survey. IET Cyber-Physical Syst Theory Appl 1(1):13–27. https://doi.org/10.1049/IET-CPS.2016.0019
62. Ibrahem MI, Badr MM, Fouda MM, Mahmoud M, Alasmary W, Fadlullah ZM (2020) PMBFE: efficient and privacy-preserving monitoring and billing using functional encryption for AMI networks. 2020 Int. Symp. Networks, Comput. Commun. https://doi.org/10.1109/ISNCC49221.2020.9297246
63. Saxena N, Choi BJ, Grijalva S (2017) Secure and Privacy-Preserving Concentration of Metering Data in AMI Networks. Available: http://icc2017.ieee-icc.org/. Accessed 30 Jan 2023
64. Seo SH, Ding X, Bertino E (2013) "Encryption key management for secure communication in smart advanced metering infrastructures", 2013 IEEE Int. Conf Smart Grid Commun SmartGridComm 2013:498–503. https://doi.org/10.1109/SMARTGRIDCOMM.2013.6688007
65. 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. https://doi.org/10.1109/ACCESS.2019.2903574
66. Parvez I, Sarwat AI, 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
67. Kebotogetse O, Samikannu R, Yahya A (2022) A concealed based approach for secure transmission in advanced metering infrastructure. IEEE Access 10:84809–84817. https://doi.org/10.1109/ACCESS.2022.3195240
68. Vijayanand R, Devaraj D, Kannapiran B (2019) A Novel Deep Learning Based Intrusion Detection System for Smart Meter Communication Network. IEEE Int. Conf. Intell. Tech. Control. Optim. Signal Process. INCOS 2019. https://doi.org/10.1109/INCOS45849.2019.8951344
69. Seferian V, Kanj R, Chehab A, Kayssi A (2018) Identity based key distribution framework for link layer security of AMI networks. IEEE Trans Smart Grid 9(4):3166–3179. https://doi.org/10.1109/TSG.2016.2628090
70. Dhanesh Menon V, Trilok Kumar J, Sabhanayagan M, Ramkumar A, Rajesh K (2019) Cyber Security for Smart Meters. IEEE Int. Conf. Intell. Tech. Control. Optim. Signal Process. INCOS 2019. https://doi.org/10.1109/INCOS45849.2019.8951407
71. John T, Hausheer D (2021) S3MP: A SCION based secure smart metering platform. Proc. IM 2021 - 2021 IFIP/IEEE Int. Symp. Integr. Netw. Manag. pp 944–949
72. Prabhakar P, et al (2022) Cyber Security of Smart Metering Infrastructure Using Median Absolute Deviation Methodology. Secur. Commun. Networks, vol. 2022. https://doi.org/10.1155/2022/6200121
73. Ian Levy (2016) The smart security behind the GB Smart Metering System. pp. 1–5. Available: https://www.ncsc.gov.uk/information/the-smart-security-behind-the-gb-smart-metering-system, https://www.ncsc.gov.uk/articles/smart-security-behind-gb-smart-metering-system
74. Jiang W, Yang Z, Zhou Z, Chen J (2020) Lightweight Data Security Protection Method for AMI in Power Internet of Things. Math. Probl. Eng., vol. 2020. https://doi.org/10.1155/2020/8896783
75. Madhu A, Prajeesha P (2021) Prevention of FDI Attacks in Smart Meter by providing Multi-Layer Authentication using ElGamal and SHA. Proc. - 5th Int. Conf. Comput. Methodol. Commun. ICCMC 2021. pp. 246–251. https://doi.org/10.1109/ICCMC51019.2021.9418464
76. "Puerto Rico Electric Power Authority (PREPA) hacked over the weekend - Cyber Defense Magazine." https://www.cyberdefensemagazine.com/puerto-rico-electric-power-authority-prepa-hacked-over-the-weekend/. Accessed 20 Mar 2024
77. Kumar M (2022) Post-quantum cryptography Algorithm's standardization and performance analysis. Array 15:100242. https://doi.org/10.1016/J.ARRAY.2022.100242
78. 2020 System and method for improved security in advanced metering infrastructure networks
79. Mohammadali A, Haghighi MS (2021) A privacy-preserving homomorphic scheme with multiple dimensions and fault tolerance for metering data aggregation in smart grid. IEEE Trans Smart Grid 12(6):5212–5220. https://doi.org/10.1109/TSG.2021.3049222
80. Farquharson J, Wang A, Howard J (2012) Smart grid cyber security and substation network security. 2012 IEEE PES Innov. Smart Grid Technol. ISGT. https://doi.org/10.1109/ISGT.2012.6175788
81. Islam N, Rahman MS HKMS-AMI: A Hybrid Key Management Scheme for AMI Secure Communication. https://doi.org/10.1007/978-981-33-4673-4_30
82. Shariat M, Safkhani M (2017) How the control over smart meters is lost in the Yan et al. lightweight AKA scheme for smart grids. 9th Int. Conf. Inf. Knowl. Technol. IKT 2017, vol. 2018-January. pp. 82–84. https://doi.org/10.1109/IKT.2017.8258622
83. Bendiab G, Grammatikakis KP, Koufos I, Kolokotronis N, Shiaeles S (2020) Advanced metering infrastructures: Security risks and mitigation. ACM Int Conf Proceeding Ser. https://doi.org/10.1145/3407023.3409312
84. Islam N, Sultana I, Rahman MS (2021) HKMS-AMI: A Hybrid Key Management Scheme for AMI Secure Communication. Adv Intell Syst Comput 1309:383–392. https://doi.org/10.1007/978-981-33-4673-4_30
85. Effah E, Owusu KB (2014) Evolution and efficiencies of energy metering technologies in Ghana. Glob J Res Eng Electr Electron Eng 14(4–5):1–9
86. Costa VLRD, Camponogara A, Lopez J, Ribeiro MV (2022) The feasibility of the CRYSTALS-kyber scheme for smart metering systems. IEEE Access 10:131303–131317. https://doi.org/10.1109/ACCESS.2022.3229521

87. Khasawneh S, Kadoch M (2021) ECS-CP-ABE: A lightweight elliptic curve signcryption scheme based on ciphertext-policy attribute-based encryption to secure downlink multicast communication in edge envisioned advanced metering infrastructure networks. Trans Emerg Telecommun Technol. 32(8) https://doi.org/10.1002/ETT.4102
88. Mattioli K, Moulinos R (2015) Communication network interdependencies in smart grid. Enisa. https://www.enisa.europa.eu
89. Karagiannis G, Pham GT, Nguyen AD, Heijenk GJ, Haverkort BR, Campfens F (2014) Performance of LTE for smart grid communications. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). vol. 8376. LNCS; pp. 225–239. https://doi.org/10.1007/978-3-319-05359-2_16/COVER
90. Patel D, et al (2016) Investigating the performance of QoS enabled LTE networks for IEC 61850 based smart grid applications. 2016 IEEE Int. Energy Conf. ENERGYCON; https://doi.org/10.1109/ENERGYCON.2016.7513965
91. "Smart Metering Via Cellular Connectivity | DigiKey."https://www.digikey.com/en/articles/cellular-connectivity-for-smart-metering. Accessed 12 Jul 2023
92. "PRIME Alliance." https://www.prime-alliance.org/. Accessed 26 Jan 2023
93. "G3-PLC Alliance |." https://g3-plc.com/. Accessed 26 Jan 2023
94. Robson S, Haddad A, Griffiths H (2018) Implementation of the Prime and G3-PLC Physical Layers in the EMTP-ATP. Proc. - 2018 53rd Int. Univ. Power Eng. Conf. UPEC. https://doi.org/10.1109/UPEC.2018.8542113
95. Zohourian A et al (2023) IoT Zigbee device security: A comprehensive review. Internet of Things 22:100791. https://doi.org/10.1016/J.IOT.2023.100791
96. Palamà I, Amici A, Bellicini G, Gringoli F, Pedretti F, Bianchi G (2023) Attacks and vulnerabilities of Wi-Fi Enterprise networks: User security awareness assessment through credential stealing attack experiments. Comput Commun 212:129–140. https://doi.org/10.1016/J.COMCOM.2023.09.031
97. Juhász K, Póser V, Kozlovszky M, Bánáti A (2019) WiFi vulnerability caused by SSID forgery in the IEEE 802.11 protocol. SAMI 2019 - IEEE 17th World Symp. Appl. Mach. Intell. Informatics, Proc. pp. 333–338. https://doi.org/10.1109/SAMI.2019.8782775
98. Seijo Simó M, López López G, Moreno Novella JI (2017) Cybersecurity Vulnerability Analysis of the PLC PRIME Standard. Secur. Commun. Networks. pp. 1–18. https://doi.org/10.1155/2017/7369684
99. Mohan V, Mathur A, Kaddoum G (2023) Analyzing Physical-Layer Security of PLC Systems Using DCSK: A Copula-Based Approach. IEEE Open J Commun Soc 4(January):104–117. https://doi.org/10.1109/OJCOMS.2022.3232753
100. Win LL, Tonyalı S (2021) Security and Privacy Challenges, Solutions, and Open Issues in Smart Metering: A Review. Proc. - 6th Int. Conf. Comput. Sci. Eng. UBMK; pp. 800–805. https://doi.org/10.1109/UBMK52708.2021.9558912
101. Chin JX, Tinoco De Rubira T, Hug G (2017) Privacy-protecting energy management unit through model-distribution predictive control. IEEE Trans Smart Grid 8(6):3084–3093. https://doi.org/10.1109/TSG.2017.2703158
102. Sunuwar R, Samal SK (2015) Elgamal Encryption using Elliptic Curve Cryptography
103. Sadhukhan D, Ray S, Obaidat MS, Dasgupta M (2021) A secure and privacy preserving lightweight authentication scheme for smart-grid communication using elliptic curve cryptography. J Syst Archit 114:101938. https://doi.org/10.1016/J.SYSARC.2020.101938
104. da Costa VLR, López J, Ribeiro MV (2022) A System-on-a-Chip Implementation of a Post-Quantum Cryptography Scheme for Smart Meter Data Communications. Sensors. 22(19). https://doi.org/10.3390/s22197214
105. Darzi S, Akhbari B, Khodaiemehr H (2022) LPM2DA: a lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. Cluster Comput 25(1):263–278. https://doi.org/10.1007/s10586-021-03387-0
106. Biswal M, Tayeen ASM, Misra S (2021) AMI-FML: A Privacy-Preserving Federated Machine Learning Framework for AMI. https://doi.org/10.48550/arxiv.2109.05666
107. de Souza MA, Pereira JL, Alves GD, de Oliveira BC, Melo ID, Garcia PA (2020) Detection and identification of energy theft in advanced metering infrastructures. Electr Power Syst Res 182:106258.https://doi.org/10.1016/J.EPSR.2020.106258
108. Williams P, Dutta IK, Daoud H, Bayoumi M (2022) A survey on security in internet of things with a focus on the impact of emerging technologies. Internet of Things 19:100564. https://doi.org/10.1016/J.IOT.2022.100564
109. Naha RK, et al (2020) Towards Secure Internet of Things : Blockchain Solutions, Challenges, and Open Issues. Blockchain Cybersecurity Priv. pp. 85–113. https://doi.org/10.1201/9780429324932-6

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.