Security and Privacy Challenges, Solutions, and Open Issues in Smart Metering: A Review

Lae Lae Win
Computer Engineering
Abdullah Gül University
Kayseri, Turkey
lae.win@agu.edu.tr

Samet Tonyalı
Electrical and Computer Engineering
Abdullah Gül University
Kayseri, Turkey
samet.tonyali@agu.edu.tr

2021 6th International Conference on Computer Science and Engineering (UBMK) | 978-1-6654-2908-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/UBMK52708.2021.9558912

***Abstract*—The traditional power grid becomes 'smart' when it is combined with the communication and information technology. Along with smart grid, the traditional meter is replaced with smart meter. Smart meters play an important role in energy consumption reporting and, thereby, billing. Besides smart meters, the smart grid communication network is composed of heterogeneous devices that are communicating through public networks. Therefore, smart metering communications are susceptible to cyber-attacks and privacy breaches which are still under debating. This paper gives a brief overview of smart grid, smart metering, and the communication networks. Then, the privacy and security requirements of the smart grid network are derived. The various kind of cyber-attacks are discussed, after that, the different schemes and approaches that have been proposed in previous papers are reviewed. Lastly, the open issues on security and privacy of smart grid metering communications are highlighted.**

***Index Terms*—smart grid, smart metering, cybersecurity, privacy**

I. Introduction

Electricity is essential for the modern society and the economy. Most countries in the world rely on electricity systems that were built many years ago. The natural resources such as wind, water, solar are transformed into electricity by bulk generations. The electric power grid is a transmission system that transfers the transformed electricity to distribution stations. The sub-stations again distribute electricity with low voltage to the end-users [1].

The power grids are not efficient and cannot offer to today's global requirements. These requirements include decarbonization, reducing environmental pollution, and energy efficiency [2]. Besides, more energy is in demand for clean water, healthcare services, smart transportation, and communications. The solution to these requirements is the Smart Grid (SG).

The smart grid is a smarter power system that will provide an improved system with environmental benefits. Its main goal is to improve the technology reliability, security, and efficiency.

The key features that the SG providing are renewable distributed energy, storage integration, grid control, and it provides energy to electric vehicles, smart appliances, smart thermostats as well as other IoT devices [3], [4]. IoTs (Internet of Things) mean the connection of a large number of devices through Internet Protocols (IPs) based solutions; i.e., it is machine to machine (M2M) communication.

The smart grid project is planning to be conducted in many countries in the future. It is an important project for both technology and economic fields. According to the market research, the SG projected market 20.83 billion USD in 2017, it is estimated to be 50.65 billion USD in 2022 [5]. The powerful growth of the SG project attracts governments, business, and academia.

In recent decades, the deployment of Information and Communication Technologies (ICTs [6]) help control and manage the smart grid so that it becomes more reliable, secure, and efficient. The smart grid is the combination of power grid and ICT. ICTs connect with smart sensors, for instance, smart meter, help in collecting smart metering data, then enable new applications. Its two main functions are billing operation and maintainability.

The Supervisory Control and Data Acquisition (SCADA) system is a centralized control system that supervises the delivery and production of energy in ICTs. Moreover, SCADA visualizes and controls the storage along with the power demand. In fact, unnecessary electricity generation is minimized by the SCADA system [5]. The system is composed of interconnected devices integrated with IPs.

Although the wireless communication is useful in SG, it may cause hazards due to the vulnerabilities [7]. The dependence on ICTs can also lead to several threats in the smart grid system. For example, an attacker can attack the steady generation of energy from a smart grid system. United States Computer Emergency Readiness Team reported that the threats are mainly focusing on energy companies [8]. The threats affect not only the network security of substations and control centers but also the customers' privacy. For example, the smart meter, an intelligent device that measures energy usage data more precisely, sends the data report over network communications that can be intercepted by snooper to invade user privacy [8].

In this paper, we focus on the security and privacy of smart grid metering communications. Also, this paper discusses potential mitigation techniques for the attacks targeting smart grid network. The rest of the paper is organized as follows. In Section II, the background of the smart grid will be discussed.

978-1-6654-2908-5/21/$31.00 ©2021 IEEE

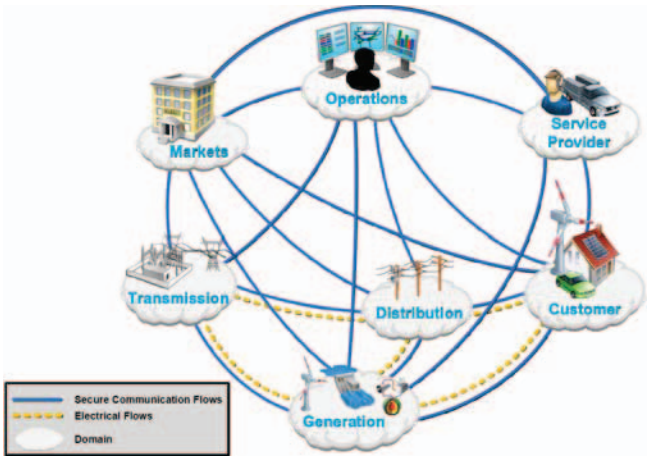

Fig. 1. Conceptual architecture framework of Smart Grid [10]

In Section III, privacy and security requirements in the SG network will be reviewed. In Section IV, security problems and existing mitigation techniques will be reviewed. In Section V, the open issues will be presented. Finally, we will conclude the paper in Section VI.

II. Background

The smart grid is composed of three main systems from the technical point of view, i.e., smart infrastructure system, smart management system, and smart protection system [9].

A. Smart Grid Infrastructure

The SG infrastructure is based on seven main domains: (i) bulk generation, (ii) energy transmission, (iii) power distribution, (iv) operation, (v) markets, (vi) service providers, and (vii) customers [8], [10]. Fig. 1 shows the interaction of roles in different smart grid domains through secure communication. Each domain involves heterogeneous elements such as buildings, organizations, and system resources.

The smart grid sends and receives the data via two-way communication. The smart grid enables the collaboration with network infrastructures such as Smart Metering Infrastructure (SMI) which not only improves the customer services but also creates a remote control from the supplier sides.

1) Smart Meters: Smart meters are typically installed near the customers' premises for computing, collecting, displaying, and transmitting the energy consumption. It is integrated with a solid-state electronic as well as a micro-controller system that contains a small memory to store the rate of energy consumption and to send the outage alert messages. The SM is also integrated with the analog to digital converter which is able to measure the current and voltage. A display unit is included in SM to display the amount of usage to the end-user so that they are capable of monitoring and controlling their energy consumption. Besides the display unit, a SM is commonly incorporated with several communication interface units, e.g., asynchronous receiver-transmitter and serial peripheral in order to connect with external devices. A real-time clock (RTC) keeps pricing information periodically to enable data analysis, billing, and time synchronization purposes.

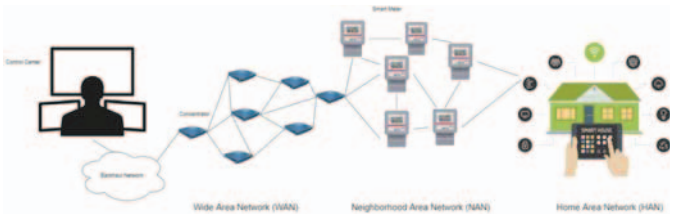

Fig. 2. Communication infrastructure in Smart Grid metering

2) Smart Metering Communication Network: The communication network in the SG environment enables to realize the smart metering networks. The communication network is in hierarchical structure, where the layers can be categorized into three classical networks based on the data rate and range as shown in Fig. 2.

a) Home Area Network: Home area network (HAN) is a network inside the customer premises. The network consists of smart appliances, lighting systems, the electric vehicles, home automation application, and building automation application. The smart meter records the actual electricity consumption reading, sends the recorded data to the data control center and executes the commands from the utility provider, in the HAN.

b) Neighborhood Area Network: Neighborhood area network (NAN) is a middle layer network that connects SMs to HAN and wide area network [11]. NAN is a complicated network which is used to transfer data from huge number of consumers to data collectors or concentrators. The requirements of NAN are higher than that of HAN. The data transfer range of NAN covers up to 100km with higher bandwidth speed and higher frequency.

c) Wide Area Network: Wide area network (WAN) is the highest layer in the smart grid that connects many data substations/concentrators and the control center. The vast amount of SMI data and signals are sent and collected through the WAN.

III. Security and Privacy Requirements

In this section, the security and privacy requirements of a smart grid communication network will be explained.

A. Security Requirements

In the past decades, power availability was the most important requirement for consumers. When the power grid is integrated with new communication technologies, availability, confidentiality and integrity have also become important [8]–[10], [12], [13]. Accountability, non-repudiation, and identification are also important objectives for smart grid security.

1) Availability: Availability is crucial for SG metering information since SM gives energy report feedback periodically [8]–[10], [12]. The main aim of availability is for ensuring the timely access, reliability, and use of information [13], [14]. The lack of availability can cause the interruption to access information in the smart meter. The availability requirements

may vary according to the type of data communication and applications. For example, the protective relaying necessitates less than 4ms latency to discover the broken lines and circuits [10]. Also, the dynamic pricing and other financial performances are obliged to be transferred in a very short amount of time.

2) Confidentiality: Confidentiality prevents the shielded data to be disclosed by unauthorized access [8], [9], [13]. In other words, confidentiality must protect the consumer's personal privacy along with the proprietary facts from being uncovered. From the consumer perspective, confidentiality is the most critical thing in that it is linked with the privacy of users and can reveal the lifestyles as well as behaviors of the end-users. Therefore, the billing information and energy usage which are delivered between the consumers and different entities should be kept confidential in order to avoid malicious purposes [3], [15].

3) Integrity: Integrity ensures that the data are protected properly from unauthorized alteration or violation. Data integrity supports data security to the SM system [16]. The integrity loss will lead to incorrect pricing, incorrect controlling of smart meter, improper energy flow, and financial losses. To maintain the integrity not only non-repudiation but also authentication is required. Non-repudiation can disrupt the abnormal performance in the smart metering network. Authentication means to prove the legitimacy of data [13].

B. Privacy in Smart Grid

In the term 'privacy' includes different ideas: the privacy of actions, privacy of thoughts and feelings. In this section, the privacy issues concern with technologies, especially, the information privacy in smart grid will be discussed. Currently, the surveys related to smart grid security focus on the privacy preserving methods.

- Privacy Information: It is related to any information of a particular person who can be identified by that information. It covers the identification number, physical, cultural, economic, locational or social identity.
- Personal Privacy: It refers to the right to manage the integrity of a person's body. It involves one's secret information like heartbeats, blood pressure, physical requirements, health problems, and the data collected by smart health devices used by that person.
- Behavioral Privacy: Every individual has the right to keep the certain personal behaviors from being disclosed to others.
- Communications Privacy: The individual may communicate with different people daily. The person should have a right to secure the communication details without being monitored, tracked or censored.

As mentioned in Section III-A, the smart meter in smart grid network transfers the energy consumption of customer periodically in every certain minutes or hours. These information are the personal information which can either reflect the individual's behavior or life patterns. Based on these data, the future activities of individuals can be predicted and applied in profiling and selling new products to customers.

IV. Security Problems and Mitigation Techniques

In this section, commonly known security problems that can be encountered in Smart Grid and existing mitigation techniques for them will be discussed.

A. Security Problems

In SG network, the Demand Response (DR) programs include exchanging the metering data from utility centers to consumers via two-way communication. There is a high probability that an intruder can interrupt and modify the signals that are transmitted through public networks. The smart grid metering, after integration with new technologies, has vulnerabilities to the attacks including interception, Denial of Services (DoS), database attack and so on. From the overview of smart grid system shown in Fig. 1, we can see that the attacks can harm both consumers and markets together with operations and utility provider domains.

1) Eavesdropping: The eavesdropping is the well-known attack to a person's privacy, i.e., attacker can intercept information packets in an unauthorized communication channel. For example, in a Man-In-The-Middle (MiTM) attack, the attacker can trace the user's energy usage and daily activity which threatens the individuals' privacy. The attacker can use sniffing, packet injections, session hijacking or SSL stripping techniques to accomplish MiTM attack. Once the attacker is able to eavesdrop in the network, he can modify the data sent in plaintext by the sender then again forward modified data to the receiver [12]. As another example, a DR program which contains the information such as date, time, location, price, and customer list is initiated through public networks. A hacker can invade or collect the information by eavesdropping. As a result, the customer in the list may be exposed to a serious privacy threat.

2) Network Interception: The backhaul IP network is used for data aggregations and controlled by most of the utility providers. The weak authentication in this network, in fact, can be a source to exploit the vulnerabilities during configuration. In addition, the IP packet encryption is not a must in, thus, IP packet can easily be interfered. As a result, the packet disruption, spoofing on the source or destination addresses, and the devices or machines may encounter misconfiguration in the network. These misconfigurations will threaten the sensitive data. For instance, an adversary can alter the destination addresses and transport packet sequence during the billing information or message transmission [17]. Therefore, the leaked data can impact on customers' privacy as the data are aggregated in the data substation which uses the backhaul IP network. The network interception attack can cause the financial loss, damage of assets and harm to household privacy.

3) Insider Attack: It is reported that the privacy issues arise when the fine-grained consumption data are sent to providers [18]. Even if the provider is reliable, the data information may be revealed to other stakeholders. For example,

the attacker has a right to access the utility databases where the consumption information is stored. In this way, theft of information can be performed by an insider.

4) Denial of Service (DoS) Attack: In this attack, the attacker may send large number of requests or packets to the control center to prevent the legitimate users from accessing.

There are some cyber attacks performed to the smart grid or traditional power grid that took place in real-world in recent few years. For example, The Ukranian power grid was attacked in 2015 [19] and 2016 [20]. Both attacks resulted in power outage. Approximately 250,000 customers were affected, and the blackout lasted for several hours.

B. Mitigation Techniques

The countermeasures of privacy invasions include non-cryptographic techniques and several identification approaches [9], [21]. In addition, several cryptographic schemes were also proposed in previous studies. Both of them aim to provide the security of smart grid and the smart meter infrastructure. Cryptographic schemes employ public and symmetric key cryptography, homomorphic encryption, and some combination of these approaches.

1) Non-Cryptographic Approaches: There are two types of non-cryptographic approaches: Battery-based load hiding and Physically Unclonable Functions.

a) Battery-Based Load Hiding (BLH): BLH, a charging-based power storage, is the most common non-cryptographic approach to protect consumers' privacy in smart metering. Chin et al. [22] proposed a power storage scheme. This scheme uses model predictive controller with power storage devices to decrease the customers' information leak by using mutual information as well as reduce energy cost by optimizing or counting of grid use. Despite this scheme is aimed to reduce the information leakage, the aim is achieved only with the expensive energy cost. Apart from this, this scheme does not scale well due to its prediction methods.

Giaconi and Gunduz [23] presented a scheme for addressing SM with renewable energy resources and a battery that partially hides consumption information. The purpose of this scheme is also to reduce the information leakage. This scheme predicts the energy management procedure using the dynamic programming. The responsibility of energy management procedure is to request the amount of energy required at a certain time to lower the leakage rate. Unfortunately, the renewable energy is wasted when the required energy load is less than generated energy.

There are demerits in BLH schemes which limit the ability and authority of smart grid. The BLH is also costly, and the repeated charging, discharging makes them to have shorter lifespan.

b) Physically Unclonable Functions (PUFs): PUFs are another non-cryptographic approach to the privacy problem. The PUFs are low cost devices and support the hardware-based authentication to prevent from impersonation attacks. The PUFs get the consumers' unclonable, unique physical entity such as fingerprints. The PUFs are used for achieving integrity, authentication, and confidentiality.

2) Cryptographic Approaches: The cryptographic approach is mainly working with encryption and the key exchanging algorithms. To achieve the authentication, Diffie-Hellman key exchange or Identity based key establishment is a good choice. For the message encryption, Data Encryption Standard (DES), Advanced Encryption Standard (AES), or Rivest-Shamir-Adleman (RSA) algorithms are suitable. The end-to-end encryption can be obtained via virtual tunnels or Internet Protocol Security (IPsec).

a) Symmetric Cryptosystem: In symmetric encryption, the same secret key is shared with two or more entities in the network to secure the channel.

To secure the SG communication, Saxena and Grijalva [24] proposed a secret key-based scheme. There are two main entities in this scheme: The Supervisory Node (SN) and Control Node (CN). A long-term string is shared between each CN and SN. This long-term string generates a secured packet whenever CN wants to communicate with SN. The packet generation is carried out before packet distribution. The long-term string also counts the successful packets in every transmission through the wireless networks. Once SN receives the packets from CN, it checks the integrity and then makes an acknowledgement. When the CN accepts the acknowledgement, both SN and CN generates a dynamic secret key to initiate the secure communication. The dynamic secret scheme is not costly since only the XOR and hashing is required. Yet, this scheme does not support sufficient security.

Liu et al. [25] advised to use Dynamic Secret-based Encryption (DSE) for SG network security. The aim of this encryption method is to secure the communication among the smart meters or devices and control center (CC). The SM and CC are agreed on a key which is used for both encryption and decryption of the data. Both of them are accomplished by low computational cost XORing method. The authors claimed that this scheme will minimize the information leaking. However, some vulnerabilities still exist in the scheme which can cause other attacks.

b) Asymmetric Cryptosystem: The asymmetric cryptosystem works with two different keys, i.e., public key and private key. The public key operates for encryption and can be shared with everyone. On the other hand, private key must be kept secret. RSA encryption is a well-known asymmetric cryptosystem using keystream of at least 1024 bits.

Based on RSA, Fan et al. [26] explored a privacy enhancing data aggregation scheme. This scheme can protect the system against the insider attack. The idea is that the customer receives the smart meter report. By encryption, the report is converted into ciphertext. The signature is computed with key pair and then sends the encrypted report to substation node. The data substation verifies the signature and the report with shared public key. The authors stated that this scheme is secured from insider attack and external attack. The integrity can also be achieved with this proposed scheme. However, the calculation may take long time, and there are thousands of

customers to send the information each day periodically (i.e. 15 mins per one report). This scheme does not seem to be practical solution in the real-world application.

Based on ElGamal encryption, Ni et al. [27] proposed a fault tolerant scheme for malfunctioning smart meters. Additionally, the authors introduced the zero-knowledge based scheme. It aims to detect the abnormal measurements induced by energy theft. The authors assured that this schemes can satisfy the privacy requirements of users and resist the differential attacks. Nonetheless, ElGamal based encryption gives the ciphertext twice as long as the original text.

c) Homomorphic Cryptosystem: The symmetric and asymmetric cryptosystems can be concluded as deterministic because the given plaintext is always converted to a unique ciphertext using the key. This lets the adversary to predict the ciphertext by performing analysis. The homomorphic cryptosystem allows the arithmetic computation on the encrypted message without knowing the secret key.

Borges et al. [28] recommended a protocol for smart metering which mainly focuses on the privacy preserving data aggregation and secured billing. To meet the users' privacy demands, the smart meter utilizes the homomorphic encryption and computes the homomorphic commitments on energy consumption data. The scheme has not been simulated or tested, so, it is not easy to analyze its usefulness.

Zhu et al. [29] proposed an efficient privacy preserving aggregation (EPPA) scheme whose system architecture is based on homomorphic cryptosystem which includes trusted authority, regional center, and operation center. In this model, the regional center collects group signatures to achieve the users' privacy and the operation center keeps the SM sensitive information without disclosing. This scheme performs well but gives the SM computational overhead.

d) Other Privacy Preserving Schemes: Vahedi et al. [30] proposed a privacy preserving data aggregation scheme based on ECC and ElGamal encryption known as Elliptic Curve Based Data Aggregation (ECBDA). The ECBDA scheme reduces the computational complexity in encryption so that it reduces the computational overhead in SMs. The proposed scheme was compared with the EPPA scheme in terms of computational overhead by using security parameters of 80, 112, 128, 192i and 256. The test results showed that ECBDA is 64 times faster than EPPA on security parameter 112. The ciphertext is 9 times shorter than that of EPPA. Also, ECBDA is 167 times faster on security parameter 128, and the ciphertext is 12 times shorter than that of EPPA.

Guan et al. [31] proposed a privacy preserving scheme based on blockchain called Privacy Preserving Blockchain Energy Trading Scheme (PP-BCETS). The model of the scheme is to establish a distributed network. The trading nodes transmit the transaction data through smart devices and that nodes jointly create a network of energy trading based on blockchain. Since most blockchain based models have the privacy exposure problem, they used Ciphertext-Policy Attribute-Based Encryption (CP-ABE) as a core encryption algorithm. They declare that their model is a lightweight distributed transaction model which can maximize the privacy protection, enhance the security and reliability. The authors compared their scheme to WePower, a blockchain-based energy trading platform, stores the information in an immutable and secure way. Test results showed that PP-BECTS is faster than WePower algorithm because the number of transactions with short confirmation time increases, while the number of transactions with long confirmation decreases.

Lardier et at. [32] proposed a Quantum Key Distribution (QKD) based protocol within open-source MOSAIK framework. The authors discussed that in the upcoming years, the quantum computers will become stronger, and the asymmetric cryptosystems may become insecure. The quantum communications will also become an important topic to the SG within several decades. The IEEE Smart Grid roadmap outlines that the security protocols currently in use are time consuming and high in computational cost, so, the quantum-based protocols can be a solution. The proposed solution, QKD, detect eavesdropping depending on the number of qubits exchanged per second. The authors used three QKD protocols, i.e., BB84, SARG04, KMB09 with one-time pad or AES-256 encryption to detect the MiTM attack rate. The authors compared the MiTM detection rate during their simulations. The results show that SARG04 protocol outperforms the rest. KMB09 performs better than BB84 when the qubit exchange rate is less than 20 per second. If the number of qubits exchanged is sufficiently large, the MiMT detection is almost perfect (approximately 100%). However, this may end up with DoS due to the repeated re-communication to the control center.

V. Open Issues

The future smart grid privacy and security mainly demand the lightweight authentication schemes. The encryption schemes such as RSA is not suitable for the SG because of the modular exponentiation that requires many CPU cycles. ECC-based schemes are relatively lightweight, but they significantly increase the size of encrypted messages even more than RSA encryption. On the other hand, AES is way more lightweight than these two cryptosystems and robust against quantum computer-based attacks. AES encryption manages the key to encrypt the blockcipher in each round. The key management would bring up a difficulty in actual implementation. Therefore, the new set of lightweight cryptosystem remains as an open issue for securing SG.

The blockchain based schemes, as mentioned in the previous section, can slow down the system when there is a large number of nodes in the network. It may take up to several minutes to create a block, so there exists the latency and energy efficiency issues.

The quantum key distribution can detect the MiTM attacks, but it is vulnerable to some other attacks such as DoS attacks. To prevent this kind of vulnerability, the quantum key distribution protocols need to be improved such that they can tolerate existence of eavesdroppers.

As mentioned above, the quantum computers will become stronger in near future, to implement a defensive method against the quantum attack is essential for SG security. Researchers proved that the lattice cryptography is anti-quantum and safe against the attacks. Although lattice cryptography is not the first choice today, researchers can use it to develop new methods or protocols. These protocols might be effective in the post-quantum era.

VI. Conclusions

In this paper, we discussed the importance of privacy and security in SG networks. The periodic information transmitting between the consumers and control center may leak the sensitive data. Moreover, the attackers can intentionally eavesdrop the information during the communication. The other kind of attacks are also discussed in this paper. If there is an attack, there should be a way to defense. There are different approaches to the attacks. The non-cryptographic techniques and cryptographic schemes are used as the mitigation techniques. Even though there are several techniques, there are new attacking ways as the technology is developing. In the future, we are planning to produce an effective model or protocol to fulfill the security and privacy requirements of Smart Gird and Smart Metering Networks.

References

[1] S. Zeadally, A.-S. K. Pathan, C. Alcaraz, and M. Badra, "Towards privacy protection in smart grid," *Wireless personal communications*, vol. 73, no. 1, pp. 23–50, 2013.

[2] D. Ahuja and M. Tatsutani, "Sustainable energy for developing countries," *SAPI EN. S. Surveys and Perspectives Integrating Environment and Society*, vol. 2, no. 1, 2009.

[3] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.

[4] A. P. Johnson, "The history of the smart grid evolution at southern california edison," in *2010 Innovative Smart Grid Technologies (ISGT)*. IEEE, 2010, pp. 1–3.

[5] "Smart grid market by software, hardware, service, and region - global forecast to 2023," https://www.marketsandmarkets.com/Market-Reports/smart-grid-market-208777577.html, 2019, accessed: 2021-02-18.

[6] J. Wu, S. Guo, H. Huang, W. Liu, and Y. Xiang, "Information and communications technologies for sustainable development goals: state-of-the-art, needs and perspectives," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2389–2406, 2018.

[7] J. J. Fritz, J. Sagisi, J. James, A. S. Leger, K. King, and K. J. Duncan, "Simulation of man in the middle attack on smart grid testbed," in *2019 SoutheastCon*. IEEE, 2019, pp. 1–6.

[8] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, 2019.

[9] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in ioe enabled smart grid advanced metering infrastructure," *Cluster Computing*, vol. 22, no. 1, pp. 43–69, 2019.

[10] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr *et al.*, "Nist framework and roadmap for smart grid interoperability standards, release 3.0," *Special Publication (NIST SP)*, 2014.

[11] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based internet of things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE wireless communications*, vol. 24, no. 3, pp. 17–25, 2017.

[12] A. Agarkar and H. Agrawal, "A review and vision on authentication and privacy preservation schemes in smart grid network," *Security and Privacy*, vol. 2, no. 2, p. e62, 2019.

[13] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Computers & Electrical Engineering*, vol. 67, pp. 469–482, 2018.

[14] M. Savi, C. Rottondi, and G. Verticale, "Evaluation of the precision-privacy tradeoff of data perturbation for smart metering," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2409–2416, 2015.

[15] S. Sultan, "Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: A survey," *Computers & Security*, vol. 84, pp. 148–165, 2019.

[16] A.-S. Khan Pathan, Z. M. Fadlullah, M. M. Fouda, M. M. Monowar, and P. Korn, "Information integrity in smart grid systems," *Information Systems*, vol. 53, no. C, pp. 145–146, 2015.

[17] Z. A. Baig and A.-R. Amoudi, "An analysis of smart grid attacks and countermeasures," *Journal of Communications*, vol. 8, no. 8, pp. 473–479, 2013.

[18] A. Paverd, "Enhancing communication privacy using trustworthy remote entities," Ph.D. dissertation, University of Oxford, 2015.

[19] "Lessons learned from a forensic analysis of the ukrainian power grid cyberattack," https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware, 2016, accessed: 2021-02-11.

[20] "Cyberattack suspected in ukraine power outage," http://www.pcworld.com/article/3152010/security/cyberattack-suspected-in-ukraine-power-outage.html, 2016, accessed: 2021-02-18.

[21] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[22] J.-X. Chin, T. T. De Rubira, and G. Hug, "Privacy-protecting energy management unit through model-distribution predictive control," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 3084–3093, 2017.

[23] G. Giaconi and D. Gündüz, "Smart meter privacy with renewable energy and a finite capacity battery," in *2016 IEEE 17th international workshop on signal processing advances in wireless communications (SPAWC)*. IEEE, 2016, pp. 1–5.

[24] N. Saxena and S. Grijalva, "Dynamic secrets and secret keys based scheme for securing last mile smart grid wireless communication," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1482–1491, 2016.

[25] T. Liu, Y. Liu, Y. Mao, Y. Sun, X. Guan, W. Gong, and S. Xiao, "A dynamic secret-based encryption scheme for smart grid wireless communication," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1175–1182, 2013.

[26] C.-I. Fan, S.-Y. Huang, and Y.-L. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial informatics*, vol. 10, no. 1, pp. 666–675, 2013.

[27] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, and X. S. Shen, "Differentially private smart metering with fault tolerance and range-based filtering," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2483–2493, 2017.

[28] F. Borges, D. Demirel, L. Böck, J. Buchmann, and M. Mühlhäuser, "A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing," in *2014 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2014, pp. 1–6.

[29] H. Zhu, F. Liu, R. Yan, and H. Li, "Pas: an efficient privacy-preserving multidimensional aggregation scheme for smart grid," *International Journal of Distributed Sensor Networks*, vol. 11, no. 10, p. 915795, 2015.

[30] E. Vahedi, M. Bayat, M. R. Pakravan, and M. R. Aref, "A secure ecc-based privacy preserving data aggregation scheme for smart grids," *Computer Networks*, vol. 129, pp. 28–36, 2017.

[31] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and privacy-preserving energy trading based on blockchain and abe in smart grid," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 34–45, 2021.

[32] W. Lardier, Q. Varo, and J. Yan, "Quantum-sim: An open-source co-simulation platform for quantum key distribution-based smart grid communications," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–6.