A Study on Privacy-Preserving Data Aggregation Techniques for Secure Smart Metering System

Farzana Kabir, Amna Qureshi and David Megías

Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC),
Center for Cybersecurity Research of Catalonia (CYBERCAT)
Av. Carl Friedrich Gauss, 5, 08860, Castelldefels, Spain
E-mail: {fkabir,aqureshi,dmegias}@uoc.edu

***Abstract*—Due to the recent growth in the use of smart meters in smart homes, secure data aggregation in a smart metering system has become a challenging issue. Data aggregation is one of the solutions for securing the consumers' data by combining the meter reading at the gateway so that the attacker cannot identify an individual user's information. This paper provides a comprehensive review of recent works on secure and privacy-preserving technologies for smart meter data collection. In addition, a brief comparative analysis of some state-of-the-art privacy-preserving data aggregation schemes is presented in terms of security and privacy requirements, and performance evaluation. This review paper points out some research challenges and unique future directions for researchers. To the best of our knowledge, no prior work has addressed issues such as managing multiple attacks and aggregation of multidimensional data (water, gas and electricity consumption data).**

Keywords: Smart meter, Data aggregation, Privacy, Digital watermarking, Encryption.

I. Introduction

The huge amount of information generated by smart meters provides an opportunity to the utility service providers to monitor and control energy consumption in real time to achieve operational accuracy [1]. A smart metering system consists of the following five components: (1) smart meter (SM): a programmable utility that generates user data and is connected with the control center and the smart home using networking technologies [2], [3]; (2) control center (CC): a central distribution system that manages the daily operations of the distribution network and is responsible for verifying the authenticity and integrity of the aggregated data and delivering respective billing data to the consumer's side; (3) data collector (DC): a service provider that collects, stores and transmits the energy consumption data from the SM. It is also responsible for aggregating user data [4]; (4) Home Area Network (HAN): a network that facilitates communication and sharing of resources among digital devices. It transfers the real-time readings of energy consumption from the SM to other entities [5]; and (5) Trusted Third Party (TTP): a trusted party responsible for registering the SM, controlling the smart metering system and generating secret keys for the system [4].

Though the fine-grained data (collected usually every 15 minutes [6]) and the power consumption requests collected by the SM offer the CC some advantages (e.g. dynamic pricing or optimal scheduling, among others), these pose a serious privacy threat to the consumers. This fine-grained metering data could expose the consumer's identity as well as his/her daily life activities that an intruder can easily use against him/her. Also, the power consumption requests used for optimal scheduling may disclose the consumer's future activity plans. Various security protection techniques have been developed in smart metering systems (such as anonymization or blind signatures); however, the data aggregation technology has been considered as a more convenient approach. Many data aggregation schemes employ cryptographic techniques (e.g. homomorphic encryption (HE), elliptic curve cryptography (ECC), digital signatures, etc.) to encrypt the consumer's energy consumption data and send the ciphertext through a trusted gateway to the CC [4]. However, these cryptographic methods are costly from a computational point of view and are vulnerable to loss of privacy. Some other schemes utilize data hiding methods, e.g. digital watermarking; however, the watermarking technology provides only one-way authentication. Therefore, it is of significant importance to develop secure and privacy-preserving data aggregation protocols for a smart metering system [1].

This survey paper highlights various outcomes of recent research works on secure and privacy-preserving data aggregation in smart meters. Our main contributions include:

- A detailed survey of recent publications including the latest works on SM's security to show how the security technology has evolved over time.
- A unique taxonomy that includes the following attributes related to the smart metering system: security and privacy requirements, threat model, classification of privacy-preserving data aggregation techniques and their subcategories, communication protocols and performance evaluation.
- A comparative analysis of the relevant state-of-the-art schemes w.r.t. the attributes defined in the taxonomy to identify their pros and cons.
- Several unique research goals that are not highlighted in previous state-of-the-art works, such as addressing multiple attacks simultaneously, multi-dimensional data security, and combining encryption with watermarking within a smart metering system to create an efficient and robust privacy-preserving data aggregation scheme.

The rest of the paper is organized as follows: Section II presents the taxonomy of secure and privacy-preserving smart metering systems. Section III surveys recent works w.r.t. the attributes defined in the taxonomy. In addition, the schemes are compared w.r.t. the attributes defined in the taxonomy. In

Section IV, we discuss challenges and open research issues. Finally, Section V concludes the paper.

II. Secure and Privacy-Preserving Smart Metering Systems

In this section, we present the proposed taxonomy to classify secure and privacy-preserving smart metering systems w.r.t. security and privacy requirements, threat model, privacy-preserving data aggregation techniques, communication protocols and performance evaluation (as shown in Fig. 1). All the attributes are briefly defined in the following sections.

A. Security and privacy requirements

1) Security Requirements: The main requirements of SM's security are authenticity (guarantee of the data to be originated from the expected sender [7]), confidentiality (an unauthorized person should not be able to gain any information related to the energy consumption of an individual user [6]), integrity (assurance of no alterations to a user data by any third party [8]), access control (the real user data can only be accessed by an authorized party [9]), availability (assurance that if an entity in the system suddenly restarts, it can re-collect the data in real time [9]) and auditability (verification of correct data received in response to a request).

2) Privacy Requirements: Different privacy requirements for assuring the secrecy of the identity and behavior of any particular user are the following: anonymity (an attacker must not be able to detect the identity of the user even if he/she can capture the consumption data [1]), pseudonymity (the user has a unique ID instead of a real name so that the attacker can not derive his/her identity), k-anonymity (re-identification of usage data in a group of k data items), and indistinguishability (if an adversary is able to capture data of two or more than two SMs, the individual's user data remains indistinguishable).

B. Threat model and its classification

An attack is an operation that enables unauthorized parties to gain illegal access to consumers' personal data, or to modify encrypted data without being recognized [3]. There can be two types of attacks in the SM communication: cyber (network attacks) and physical attacks.

Physical attacks have the ability to cause physical damage to the communication links or smart devices [10] by aggressive destruction of SM terminals [3], such as node tampering (capturing the SM and tampering with its circuit) [11], power loss (sudden loss of power in the communication channel), load rejection (random load loss in the smart metering system), malicious code injection (injecting malicious code for compromising the SM) and malicious node insertion (inserting malicious node by impersonating a legitimate node [11]).

Possible cyber attacks include eavesdropping (sniffing data traffic of the SM system by an intruder), impersonation (an active type of attack in which the attacker captures some type of authentication traffic to authenticate to the service provider), masquerading (a passive attack in which an attacker uses a fake identity to pretend as an internal entity) [4] or replay attack (a network attack in which the SM's report is re-sent or delayed maliciously). Another two common attacks are man-in-the-middle (MIMA) (an attacker intercepts the messages sent between the SM and the utility service provider and attempts to modify the usage data [4]), and denial-of-service (DoS) attack (an attacker sends fake requests to decrease the availability of the system with an intended purpose [2]).

C. Data aggregation in smart metering systems

Data aggregation is one of the best concepts to protect users' fine-grained data from the middle nodes of the communication channel as well as other entities. It is a challenging task to develop a strong privacy-preserving aggregation scheme that could guarantee user privacy, security, and integrity of consumer's personal data against all the attacks mentioned in Section II-B. There are three types of aggregating methods. The first type of aggregation method is "aggregate message authentication code (MAC) and aggregate signature", in which the aggregate MAC requires a secret key between the data generator and the aggregator to verify integrity, while the aggregate signature can verify the integrity by accessing the public key. However, this method is unsuitable for resource-constrained applications due to the use of homomorphic signature [12]. The second method is "privacy-preserving and verifiable data aggregation", which allows multiple users to send encrypted data periodically and verifies data integrity without disclosing any other information. It is a multi-dimensional aggregation technique suitable for resource-constrained system devices in a wireless sensor network (WSN). A drawback in this type of aggregation method is the lack of security against all kind of internal attacks (such as impersonation or masquerading, among others) [13]. The third type, "privacy-preserving data aggregation" (P2DA), reduces the energy consumption at each node by lowering the communication overhead while preserving the privacy of sensor data at the same time. This P2DA method is suitable for guaranteeing data integrity as well as protecting the system from both internal and external attackers in a recourse constrained system [12]. A large number of P2DA techniques have been developed in recent years due to its effectiveness. The most commonly used security mechanisms in P2DA are cryptographic and data hiding methods.

Among the cryptographic techniques, HE enables the numerical modification of encrypted data without needing to decrypt it [3]. HE algorithms exist in both partial (PHE) and full forms (FHE) [14]. ECC is another cryptographic method, based on elliptic curves [15], that can ensure a similar level of security as a traditional public-key cryptography using a much shorter key [16]. Another public-key cryptographic primitive, Digital Signature Algorithm (DSA), is used in data aggregation schemes to provide source authentication and integrity of data to be aggregated. These signatures can be generated using any public-key cryptosystem. Additionally, a new cryptographic technique, signcryption, can be used in P2DA schemes to perform the functions of digital signature and encryption in a single step. There are some other cryptographic algorithms such as symmetric (e.g.Advanced Encryption Stadard (AES)) or public-key/asymmetric key (e.g. Rivest–Shamir–Adleman (RSA)) algorithms. A data hiding technique used in P2DA schemes can be based on digital watermarking, which is proved to be convenient in terms of complexity and costs [17].

HE-based data aggregation schemes have a few drawbacks, such as not being able to defend privacy attacks through

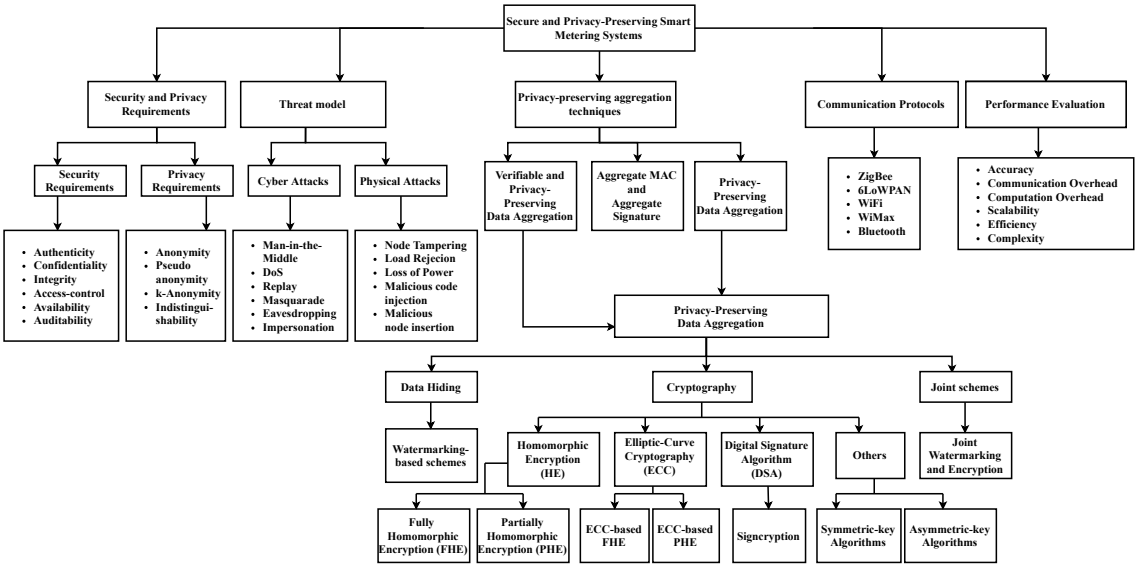

Fig. 1: Taxonomy of Secure and Privacy-Preserving Smart Metering Systems

multiple user collusion or user-aggregator collusion [18], and computational complexity due to the large key size. As with ECC, the public key needed for Elliptic Curve Digital Signature Algorithm (ECDSA) is about twice the size of the security level needed. Similarly, watermarking-based aggregation schemes suffer from a major drawback, i.e. watermarking provides a one-way authentication; however, for a secure SM, a two-way authentication is required. In order to solve these issues, combining cryptographic and data hiding techniques together or performing both simultaneously can be a good solution. Such joint watermarking and encryption schemes are being suggested by several researchers.

D. Smart Meter Communication

The SM allows a two-way communication among its entities. Hence, the communication technology needs much focus, since each SM must be secure and user privacy needs to be guaranteed while transmitting the collected information [19]. This communication can either be wireless or through a fixed wire. Here, wireless communication is a better option for data transfer and automatic configuration of a network [8]. IEEE 802.15.4 is considered the best communication standard for the smart metering network due to its efficiency, low cost, and flexible nature [8].

There are several protocols that are based on the IEEE 802.15.4 standard. However, Zigbee and 6LoWPAN are noticed to be commonly used because of the compatibility with IPv6-based networks and increased battery lives [2]. Two most suitable protocols used for communication in the smart metering system are described below:

- ZigBee: The network infrastructure that is required for WSN applications can be provided by a standard based protocol known as ZigBee, which is the communication protocol mainly based on IEEE 802.15.4. A ZigBee mesh network is suitable for smart metering applications because of its inherent redundancy, self-configuring and self-healing capabilities [19]. Within a ZigBee network, the SM data is aggregated in the form of packets within a specific time interval incurring very low communication overhead [20].
- 6LoWPAN: It stands for IPv6 over Low power Wireless Personal Area Network, which is a standard authorized by the Internet Engineering Task Force (IETF) in 2007. This protocol is used for the optimization of IPv6 for use with low-power and low-bandwidth communication technologies, such as the IEEE 802.15.4 [19]. It significantly reduces the computational overhead and data redundancy.

One advantage of 6LoWPAN over Zigbee is its ability to communicate with any other IP-enabled devices. Moreover, data transmission is much faster and the stack size is almost three times smaller in 6LoWPAN as compared to Zigbee.

E. Performance Evaluation

The main criteria to evaluate the performance of any smart metering security scheme consists of the following metrics: accuracy (the operation being correct), computational (overall time spent in installation and other delays) and communication (overall massages exchanged during system operations) overheads, efficiency (overall energy used to execute an operation [21]), robustness (strong performance in all conditions [17]), scalability (ability to process similarly when the system nodes are increased or updated [22]), and complexity (total amount of resources required to run the system).

III. Survey on Smart Metering Systems

In this section, we briefly review some of the recent research works w.r.t. the attributes presented in Section II-C, and discuss their contributions, outcomes, and limitations.

A. Literature review

In 2014, Yoon et al. [23] proposed a signature-based security technique for data aggregation that uses arithmetic properties of the complex numbers. This method is resource efficient and can guarantee data integrity, but it did not show how other security parameters were satisfied such as authenticity or access control. A lightweight lattice-based homomorphic

cryptosystem was employed in [6] to encrypt user's consumption data as noisy lattices. The proposed system highlights the fact that, when the number of SMs are increased in a network, HE schemes suffer from lack of flexibility. Chen et al. [17] proposed a privacy protection method for the WSN using wavelet dual watermarking that can prevent tampering and packet loss and significantly provides data integrity in SM. Since the proposed scheme has employed two different watermarking techniques simultaneously, time delay and cost effectiveness need to be analyzed.

Li (2017) developed a privacy-preserving multi-subset data aggregation (PPMA) scheme in which the sum of users' energy consumption is divided into multiple subsets, which are aggregated to preserve the privacy of SM's data by utilizing the Paillier homomorphic cryptosystem [24]. However, this scheme can be computationally costly. To solve the problem of large processing power, Vahedi et al. (2017) proposed an ECC-based data aggregation (ECBDA) scheme, which employs homomorphic mapping together with a blinding factor to preserve privacy against internal attackers [15]. This method is suitable for a resource-constrained SM, but is unable to aggregate multi-dimensional data. Another solution, proposed by Yan (2017), contains a lightweight digital watermarking framework that employs two different approaches of watermarking and public-key infrastructure (PKI) [21]. Despite having low computational complexity, it can secure data in the network of a smart grid with a low operational expense. AES encryption is used by Song et al. [9] to design chaos-based encryption and Message Authentication Codes (MAC) for a smart metering system. In 2015, Panah et al. developed a secure aggregation method by adopting a spread spectrum (SS)-based watermarking scheme for a data stream that successfully verifies data integrity [22]. However, this scheme has a high processing time. In 2017, this scheme was modified to ensure trustworthiness in data aggregation over a big data stream. However, the inconsistent sampling rate problem was not solved [25].

Tonyali [14] developed an algorithm based on FHE and secure multiparty computation to secure SM's reading data. This scheme resolves a packet reassembly problem and effectively protects the network from the replay attack and eavesdropping. However, this method cannot significantly outperform the efficiency of PHE. An efficient P2DA scheme is proposed by Braeken et al. (2018), which protects the security and privacy of usage data inside SM, DC and CC, such that these cannot access the aggregated meter reading. This method adopts ECC, symmetric encryption, and one-way hashing functions to provide identity-based mutual authentication and supports dynamic billing (real time billing) [13]. Unfortunately, this scheme fails to provide anonymity since its main goal is to achieve efficiency.

Bhanse et al. proposed a novel authentication approach using a variable random function (VRF) instead of digital signature for authentication. The proposed VRF uses ECC and preimage attacks are prevented [7]. A mutual privacy-preserving authentication scheme and a key-exchange algorithm are designed by S. Garg et al. The proposed scheme utilizes fully-hashed menezes-qu-vanstone (FHMQV) and ECC to secure the communication in SMs and a NAN gateway. Both schemes support mutual authentication and can resist various attacks, such as DoS, replay attacks, impersonation, or MIMA [1], [7]. Karampour et al. (2019) presented an approach for smart grid data aggregation based on AV-net mask and the Paillier cryptosystem to preserve the privacy in a smart metering system. The proposed scheme has focused on the GLP (a cryptographic scheme for group location privacy) approach, and provides security against several attacks including collusion of $n-1$ SMs [10]. It does not need any secure channel for transmission and, hence, it has a low computational overhead. However, the overall communication cost is not less than the existing state-of-the-art research works. Zhang et al. (2019) presented a distributed temporal and spatial aggregation scheme that can protect the system from internal and external attacks even if the CC tries to decrypt the homomorphically encrypted SM's readings. A shortcoming of this scheme is its inability to provide essential functionalities, such as dynamic billing [3]. Guan (2019) used the Paillier cryptosystem to develop a P2DA scheme based on secret sharing that can resist differential attacks and guarantee user's privacy [26]. In addition, fault tolerance is considered in this scheme. The authors suggest combining data privacy and dynamic billing as a possible future work. Till now, the existing error rate can affect the billing data which needs to be solved. Sui et al. (2019) proposed a signcryption protocol using the privacy-streaming aggregation algorithm as the basic encryption method. The authors designed a signature mechanism based on the timing of the metering data transmission that significantly improves the homomorphic feature of the encryption, where SMs can aggregate consumption data in a privacy-preserving and secure manner [4]. A major drawback of this scheme is that the computational and communication overheads have not been analyzed. Another attribute identity-based ring signcryption algorithm is designed by Zhang (2019), which allows the CC to verify the trustworthiness of the SM by analyzing the consumers' fine-grained data without any privacy leakage [18]. However, trustworthiness needs to be guaranteed when the SM is updated.

Li et al. (2020) presented SecGrid, a secure SGX enabled smart grid scheme that ensures the privacy of a user data by applying AES encryption in the SMs. This method is secure against malicious attackers, but it does not provide a two-way authentication that is needed for billing and load forecasting operations [27]. Also, a public-key cryptographic system, such as RSA is used in security mechanisms for P2DA [21], [28]. In [28], a practical group blind signature is introduced to solve the issue of anonymous authentication's inability to detect malicious attackers. This method allows CC to identify any potential corrupted DC and SM. In addition, scalability and anonymous authentication are provided, but mutual authentication is not addressed.

B. Comparative Analysis

After the in-depth description of the state-of-the-art research works in Section III-A, here in this section, we compare these schemes w.r.t. the taxonomy defined in Section II.

Among the three popular P2DA techniques, cryptographic methods are the most widely used in a smart metering system. A small number of research works have been conducted based on data hiding techniques and a very few researchers have used joint techniques. Watermarking, especially dual

watermarking, is mostly preferred by the researchers [17], [21] as a data hiding method. Among the cryptographic methods, homomorphic and ECC-based schemes are more popular than symmetric-key algorithms. From previous research works, it is evident that symmetric-key algorithms cannot protect the system from various attacks [23] and do not provide the required user privacy, which can be provided by HE or ECC-based schemes. Signcryption is the only joint cryptographic technique that has been proposed for a smart metering system till now [4], [18]. Joint watermarking and encryption-based schemes have not been used in state-of-the-art of P2DA schemes.

Most of the compared methods have addressed integrity, authenticity and confidentiality. Very few schemes provide guarantees of security requirements, such as availability [27] and access control [9], [18] of the usage data, and privacy requirements like anonymity [15], [1], [18] and indistinguishability [3]. In terms of security against attacks, a few digital watermarking-based P2DA techniques provide resistance against packet loss [17], [21]. The performance of the SM's security mechanisms depends on the communication protocol, which has not been addressed by the compared schemes, except for the systems proposed in [6], [13], [15], and [27].

A noticeable fact is that almost all the schemes have conducted simulation-based analysis rather than real-world experimentation. Most of these schemes have shown satisfactory performance in terms of computational and communication overheads. The ECBDA [15] and the PPMA schemes [24] are more efficient in terms of computational overheads as compared to the other schemes. The schemes based on the signcryption [4], [9] incurred less communication overheads as compared to the other schemes. In view of the time execution of different P2DA methods, the signcryption protocol in [18] and the signature-based protocol in [23] have much lower execution time. From this comparison in terms of performance evaluation, it can be said that signcryption is more efficient in terms of time complexity.

IV. Limitations and Open Research Issues

This section summarizes the limitations and open research issues of privacy-preserving and secure data aggregation for smart metering systems.

A. Limitations

It is obvious, from the literature review, that sufficient importance has not been given on fulfilling the privacy requirements while satisfying the security properties. Additionally, physical attacks, such as malicious code injection or malicious node insertion, have not been addressed by the recent studies. The existing trade-off between usability and user privacy is a vital problem, which is not highlighted in most of the research works. A relevant drawback of the existing schemes is that they do not mention about the suitable communication protocols, which is a very important issue. Moreover, mutual authentication is not addressed by most of the compared schemes, except for the ECC-based schemes proposed in [1], [7], [29]. The comparative analysis in terms of the performance evaluation exposes the fact that none of the compared schemes have been evaluated under real world conditions. Moreover, most of the research works have not focused on energy consumption and computational complexity, which makes it difficult to compare the efficiency of the schemes.

B. Open research issues

By reviewing and comparing the recent research works related to the SM's secure and privacy-preserving data aggregation, we can identify some future research directions.

- The previous works have only been evaluated in either open-source or customized simulators to conduct performance analysis. These experiments need to be carried out in the real world to evaluate their performance.
- To provide rich functionalities, such as dynamic billing or energy feedback, a two-way authentication is necessary to guarantee better security in the P2DA scheme. Future research works must provide mutual authentication in order to guarantee proper security and privacy.
- A challenge for the future researchers is to develop a scheme that can protect privacy of multi-dimensional data, such as water, gas and electricity [15] and the SM data from multiple attackers simultaneously.
- In order to develop a reliable security mechanism, the system model should address the suitable communication protocol. This issue needs to be considered for future real-world implementation of P2DA schemes.
- In the future, joint watermarking and encryption schemes can be designed to achieve privacy-preserving data aggregation by combining any advanced homomorphic encryption algorithm with a robust watermarking technique.

In a nutshell, we can conclude that there are several aspects which require improvement in smart metering applications, and therefore, more efficient, secure and robust data aggregation mechanisms must be developed.

V. Conclusion

The privacy of smart metering systems has been in the research limelight for a long period and still, improvement in this area is being continued because the smart metering architecture plays a major role in a smart grid system. Mainly, privacy and security are preserved by applying privacy-preserving data aggregation techniques. In this survey paper, we have analysed the recent research works related to privacy-preserving data aggregation in a smart metering system, and found out that most of the privacy-preserving schemes have employed HE, while a few have utilized digital watermarking. Some of these works have used basic HE, while others have proposed modified versions of HE. A few researchers have proposed dual watermarking schemes, while some others proposed the use of signcryption that simultaneously performs the functions of both digital signature and encryption. Each of these privacy-preserving schemes have focused on different privacy and security requirements, and have diverse performance evaluation criteria. In this work, we have defined a taxonomy to classify the state-of-the-art research works followed by a brief literature review along with a comparative analysis to identify their limitations and open research issues. The proposed taxonomy allows to guide the researchers in the development of secure and efficient P2DA schemes. Finally, some significant research challenges of P2DA techniques are discussed as future research directions.

REFERENCES

[1] S. Garg, K. Kaur, G. Kaddoum, J. J. Rodrigues, and M. Guizani, "Secure and lightweight authentication scheme for smart metering infrastructure in smart grid," *IEEE Transactions on Industrial Informatics*, 2019.

[2] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[3] L. Zhang, J. Zhang, and Y. H. Hu, "A privacy-preserving distributed smart metering temporal and spatial aggregation scheme," *IEEE Access*, vol. 7, pp. 28 372–28 382, 2019.

[4] Z. Sui and H. de Meer, "An efficient signcryption protocol for hop-by-hop data aggregations in smart grids," *IEEE Journal on Selected Areas in Communications*, 2019.

[5] A. M. Khattak, S. I. Khanji, and W. A. Khan, "Smart meter security: Vulnerabilities, threat impacts, and countermeasures," in *International Conference on Ubiquitous Information Management and Communication*. Springer, 2019, pp. 554–562.

[6] A. Abdallah and X. S. Shen, "A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 396–405, 2016.

[7] P. Bhanse, B. Mishra, and D. Jena, "A novel smart meter authentication scheme for secure smart grid communication," in *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*. IEEE, 2019, pp. 1275–1279.

[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] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for iot applications in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1844–1852, 2017.

[10] A. Karampour, M. Ashouri-Talouki, and B. T. Ladani, "An efficient privacy-preserving data aggregation scheme in smart grid," in *2019 27th Iranian Conference on Electrical Engineering (ICEE)*. IEEE, 2019, pp. 1967–1971.

[11] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17–25, 2020.

[12] N. H. Tran, R. H. Deng, and H. Pang, "Privacy-preserving and verifiable data aggregation." in *SG-CRC*, 2016, pp. 115–122.

[13] A. Braeken, P. Kumar, and A. Martin, "Efficient and privacy-preserving data aggregation and dynamic billing in smart grid metering networks," *Energies*, vol. 11, no. 8, p. 2085, 2018.

[14] S. Tonyali, K. Akkaya, N. Saputro, A. S. Uluagac, and M. Nojoumian, "Privacy-preserving protocols for secure and reliable data aggregation in iot-enabled smart metering systems," *Future Generation Computer Systems*, vol. 78, pp. 547–557, 2018.

[15] 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.

[16] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.

[17] Q. Chen and M. Xiong, "Dual watermarking based on wavelet transform for data protection in smart grid," in *2016 3rd International Conference on Information Science and Control Engineering (ICISCE)*. IEEE, 2016, pp. 1313–1316.

[18] S. Zhang, T. Zheng, and B. Wang, "A privacy protection scheme for smart meter that can verify terminal's trustworthiness," *International Journal of Electrical Power & Energy Systems*, vol. 108, pp. 117–124, 2019.

[19] Z. Lipošćak and M. Bošković, "Survey of smart metering communication technologies," in *Eurocon 2013*. IEEE, 2013, pp. 1391–1400.

[20] K. Dong, "Performance and fairness enhancement in Zigbee networks," http://resolver.tudelft.nl/uuid:3c0a06cb-527d-4934-b63c-979123d69d47, 2011, accessed on February 19, 2021.

[21] X. Yan, L. Zhang, Y. Wu, Y. Luo, and X. Zhang, "Secure smart grid communications and information integration based on digital watermarking in wireless sensor networks," *Enterprise information systems*, vol. 11, no. 2, pp. 223–249, 2017.

[22] A. S. Panah, R. van Schyndel, T. Sellis, and E. Bertino, "In the shadows we trust: A secure aggregation tolerant watermark for data streams," in *2015 IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2015, pp. 1–9.

[23] M. Yoon, M. Jang, H.-I. Kim, and J.-W. Chang, "A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 10, no. 1, p. 272537, 2014.

[24] S. Li, K. Xue, Q. Yang, and P. Hong, "Ppma: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 462–471, 2017.

[25] A. S. Panah, R. van Schyndel, and T. Sellis, "Towards an asynchronous aggregation-capable watermark for end-to-end protection of big data streams," *Future Generation Computer Systems*, vol. 72, pp. 288–304, 2017.

[26] Z. Guan and G. Si, "Achieving privacy-preserving big data aggregation with fault tolerance in smart grid," *Digital Communications and Networks*, vol. 3, no. 4, pp. 242–249, 2017.

[27] S. Li, K. Xue, D. S. Wei, H. Yue, N. Yu, and P. Hong, "Secgrid: A secure and efficient sgx-enabled smart grid system with rich functionalities," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1318–1330, 2019.

[28] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 29–39, 2020.

[29] D. Abbasinezhad-Mood, A. Ostad-Sharif, M. Nikooghadam, and S. M. Mazinani, "A secure and efficient key establishment scheme for communications of smart meters and service providers in smart grid," *IEEE Transactions on Industrial Informatics*, 2019.

[30] P. Gope, "Pmake: Privacy-aware multi-factor authenticated key establishment scheme for advance metering infrastructure in smart grid," *Computer Communications*, 2020.

[31] D. Engel and G. Eibl, "Wavelet-based multiresolution smart meter privacy," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1710–1721, 2015.

[32] R. Gabriel, J. Matthes, H. B. Keller, and V. Hagenmeyer, "Detection and localization of manipulated smart meters using super state hidden markov models," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2019, pp. 1–7.

[33] Y. Gui, A. S. Siddiqui, S. M. Tamore, and F. Saqib, "Security vulnerabilities of smart meters in smart grid," in *IECON 2019-45th Annual Conference of the IEEE Industrial Electronics Society*, vol. 1. IEEE, 2019, pp. 3018–3023.

[34] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 5820–5830, 2017.

[35] Y. Sun, L. Lampe, and V. W. Wong, "Smart meter privacy: Exploiting the potential of household energy storage units," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 69–78, 2017.

[36] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE transactions on information forensics and security*, vol. 12, no. 9, pp. 2227–2241, 2017.

[37] M. T. Ahvanooey, Q. Li, X. Zhu, M. Alazab, and J. Zhang, "Anitw: A novel intelligent text watermarking technique for forensic identification of spurious information on social media," *Computers & Security*, vol. 90, p. 101702, 2020.

[38] S. Sultana, M. Shehab, and E. Bertino, "Secure provenance transmission for streaming data," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 8, pp. 1890–1903, 2012.

[39] M. Burunkaya and T. Pars, "A smart meter design and implementation using zigbee based wireless sensor network in smart grid," in *2017 4th International Conference on Electrical and Electronic Engineering (ICEEE)*. IEEE, 2017, pp. 158–162.

[40] S. C. Lu, Q. Wu, and W. K. Seah, *Quality of service provisioning for smart meter networks using stream control transport protocol*. School of Engineering and Computer Science, Victoria University of Wellington, 2012.

[41] B. Tiwari, C. M. Upadhyay, S. Agarwal, and S. Udupa, "Wireless communication technologies for smart metering-opportunities and challenges," in *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2018.

[42] A. Alghamdi, M. Alshamrani, A. Alqahtani, S. S. A. Al Ghamdi, and R. Harrathi, "Secure data aggregation scheme in wireless sensor networks for iot," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2016, pp. 1–5.

[43] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.

[44] J. Hu, J. Luo, Y. Zhang, P. Wang, and Y. Liu, "Location-based data aggregation in 6lowpan," *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1–9, 10 2015.

[45] J. Wright, "Killerbee: practical zigbee exploitation framework," in *11th ToorCon conference, San Diego*, vol. 67, 2009.