energies

MDPI

Review

Fault-Tolerant Secure Data Aggregation Schemes in Smart Grids: Techniques, Design Challenges, and Future Trends

Hayat Mohammad Khan [1], Abid Khan [2], Bashar Khan [1] and Gwanggil Jeon [3,4,*]

[1] Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan
[2] College of Science and Engineering, University of Derby, Derby DE22 1GB, UK
[3] Department of Embedded Systems Engineering, Incheon National University, Incheon 22012, Republic of Korea
[4] Energy Excellence & Smart City Lab., Incheon National University, Incheon 22012, Republic of Korea
* Correspondence: gjeon@inu.ac.kr

Abstract: Secure data aggregation is an important process that enables a smart meter to perform efficiently and accurately. However, the fault tolerance and privacy of the user data are the most serious concerns in this process. While the security issues of Smart Grids are extensively studied, these two issues have been ignored so far. Therefore, in this paper, we present a comprehensive survey of fault-tolerant and differential privacy schemes for the Smart Gird. We selected papers from 2010 to 2021 and studied the schemes that are specifically related to fault tolerance and differential privacy. We divided all existing schemes based on the security properties, performance evaluation, and security attacks. We provide a comparative analysis for each scheme based on the cryptographic approach used. One of the drawbacks of existing surveys on the Smart Grid is that they have not discussed fault tolerance and differential privacy as a major area and consider them only as a part of privacy preservation schemes. On the basis of our work, we identified further research areas that can be explored.

Keywords: Smart Grid; fault tolerance; differential privacy; privacy preserving; data aggregation

Citation: Khan, H.M.; Khan, A.; Khan, B.; Jeon, G. Fault-Tolerant Secure Data Aggregation Schemes in Smart Grids: Techniques, Design Challenges, and Future Trends. *Energies* **2022**, *15*, 9350. https://doi.org/10.3390/en15249350

Academic Editors: Yun Yang, Sidun Fang and Liang Liang

Received: 23 October 2022
Accepted: 28 November 2022
Published: 9 December 2022

1. Introduction

The Smart Grid (SG) refers to the integration of power system engineering, communications, and information technology [1]. It offers the most robust, efficient, and trustworthy energy system. The smartness of the system provides the additional facility of peer-to-peer or bi-directional communication [2] and intelligently satisfies the energy demands in real-time with flawless transmission and distribution of electric energy from the suppliers to the home users. It enables the customers to view their current electricity usage through a web interface. In comparison to the traditional power grid, the SG has made power generation, transmission, and distribution to customers more robust, flexible, and effective through the integration of various technologies. Important components of the SG are the cloud control centre (CCC), gateway (GW)/fog node (FN), users (U), and smart meter (SM). SMs are installed at customer premises and submit their usage data through intermediate nodes (GW/FN) to the CCC in a secure manner. At the CCC, overall usage is calculated. At the SG level, numerous analytics relating to demand–response, forecasting, and load management are carried out based on consumption data. Figure 1 shows the high-level model of the SG.

The SG's physical infrastructure is vulnerable to a variety of cyber security attacks. Security incidents related to facility disturbances threaten the lives of citizens and even compromise national security [3]. Researchers have been studying various areas of the SG, such as the physical setup, communication technologies, legal issues, reliability, early diagnosis of failures and their recovery, demand–response management, data aggregation capability, cyber security, and customer privacy [3,4].

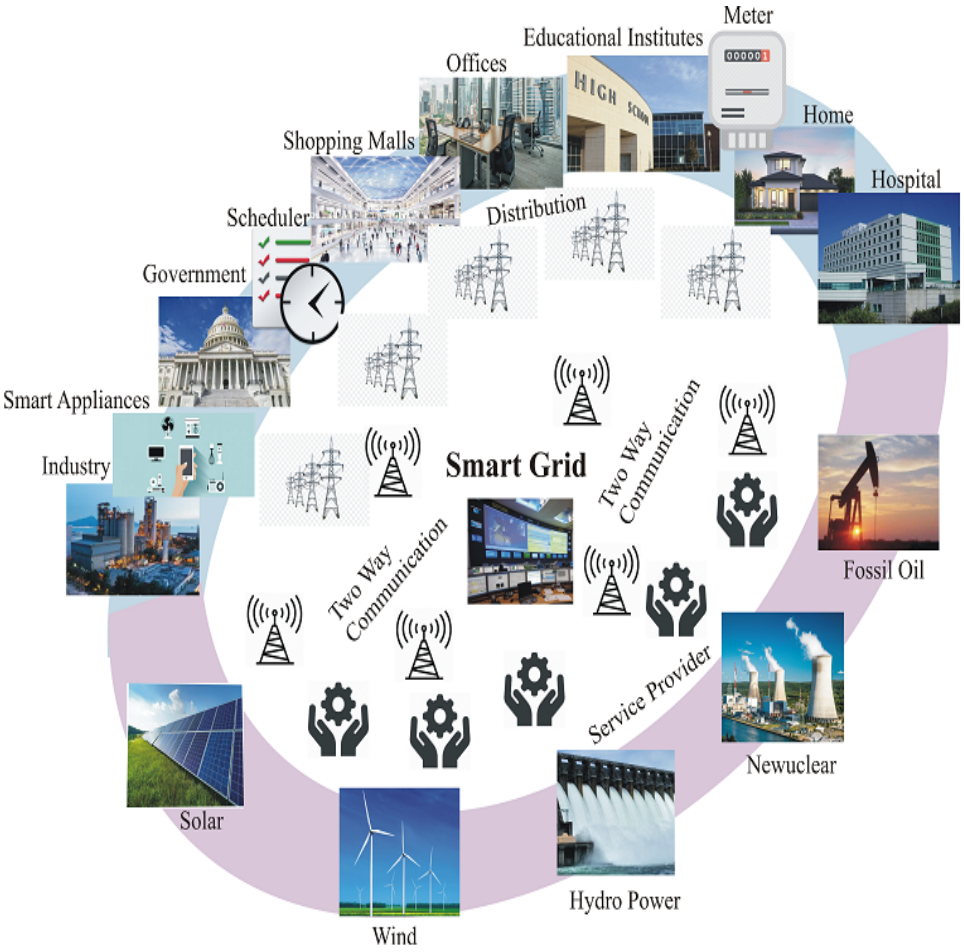

Figure 1. Model of a Smart Grid.

The two types of data collected by SG technologies are personally identifiable information and consumer-specific energy usage data. Submitting data at regular intervals in plaintext to the CCC results in privacy issues. Through secure data aggregation and by placing an intermediate gateway server (GW) between the SM and CCC, privacy and communication overhead can be reduced significantly [5]. During data aggregation, some SMs or GW/FN can drop or malfunction. If some SMs are malfunctioning or faulty and do not submit their data, this will introduce a delay in data aggregation activity, and subsequently, the CCC will not be able to calculate electricity usage; this will impact the SG operations with respect to demand–response and load management. In a fault-tolerant secure data aggregation (FTSDA) scheme, if there are some faulty SMs, this will not impact data aggregation activity [6]. This survey discusses the existing literature related to secure data FTSDA schemes in SGs.

Some of the existing SDA schemes achieve FT by using: (i) the addition of subtle strings [7], (ii) dummy text addition [8], (iii) the isolation of malfunctioning meters [9], (iv) future ciphertext [10], (v) the most recent reading stored at the FN level [11], and (vi) error detection through paring [12]. In Figure 2, FT achieved by various schemes during data collection in SG is presented.

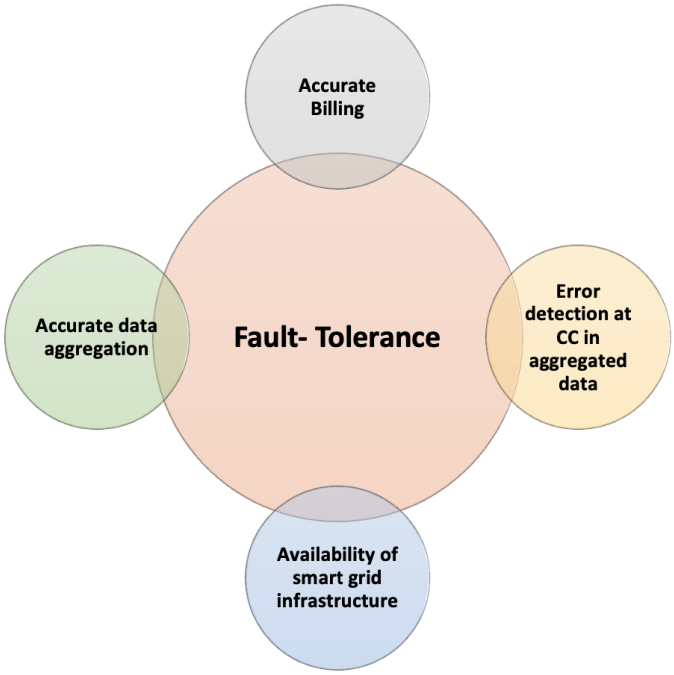

Figure 2. Fault tolerance in the Smart Grid.

In the Smart Grid, one of the important concerns is customer data. If these data are shared with the wrong entities, they may produce bad results for the customer. From those data, an intruder can check the lifestyle of the customer and his/her presence at the premises. To ensure the confidentiality of customer data, they are encrypted through the appropriate security protocol before submitting them to the aggregator. However, one challenging problem is that the aggregation scheme may suffer from a differential attack [7]. In a differential attack, the CCC can infer the customer's private data from two datasets differing by one element. To avoid this situation, differential privacy was first proposed by Dwork [13]. In this method, appropriate noise is chosen from a geometric, Laplace, or binomial distribution and added to the aggregation data to perturb them. This perturbation makes the output indistinguishable from similar datasets. In a Smart Grid, noise addition activity can be performed at the smart meter level, aggregator level, or both levels. Note that, if there are malfunctions at the users, the utility results may vary due to noise addition.

Contribution: In this work, we provide a comprehensive study of all the main techniques used in FTSDA schemes in Smart Grids as of the writing, and we cover the following:

1. We identify the key security and performance characteristics of SDA schemes in SGs that enable users to share their data with SG operators with confidence.
2. A detailed taxonomy of FTSDA schemes in SG schemes is provided.
3. We provide a discussion on how FTSDA can be achieved by using asymmetric and symmetric cryptography techniques.
4. We identify future directions and trends in SDA that should be focused on by the research community.

Organization: The rest of the paper is organized as follows: In Section 2, the requirements of the fault-tolerant (FT) schemes are presented. In Section 3, security attacks on fault-tolerant aggregation schemes in SGs are discussed. In Section 4, a comprehensive taxonomy is presented for FT-based secure aggregation schemes in SGs. In Section 5, a comparative analysis of existing SG aggregation schemes having FT and differential privacy is provided. Finally, in Section 6, we discuss the design challenges and future trends.

2. Requirements

In this section, secure aggregation schemes for the requirements of SGs with respect to FT, security properties, and performance properties are discussed.

2.1. Fault Tolerance

FT is a system property that ensures that the system continues to function properly even if one or more of its components fail. Graceful degradation refers to the ability of a system to maintain functionality when certain components of a system break down [3]. FT in SGs can be used in various stages:

- The DCC should be efficient and capable of decrypting the aggregation of working SMs. If there are some faulty SMs, this has no big impact on the overall usage calculation.
- Although the DCCs (servers) are robust and reliable, sometimes, they malfunction or shut down to protect against certain threats.
- Due to the low cost and running in an unprotected environment, SMs are prone to failures. They are also concerns for communicating over an unreliable network channel, and sometimes, they may not forward the user's data. In order to properly execute the real-time data monitoring and analysis activity at the grid level, the metering system should be able to aggregate the measurements of the remaining functional SMs when one or more of them fail to report.

2.2. Security Requirement

To ensure customer trust, the secure aggregation scheme must possess the following properties:

1. **Confidentiality:** Unauthorized entities must not be able to observe the data pattern to know about the metering data, i.e., which types of electric appliances are used by customers at home at a particular time [14–16].
2. **Integrity**: Integrity provides assurance that the data message has not been altered or modified without proper authorization. Without integrity checks, false data may be injected, which leads to incorrect information gathering at the CCC. As a result, the CCC may make the wrong decisions based on the wrong information regarding demand and response, forecasting, and billing [6,17].
3. **Authentication:** During data submission, the SM, FN, and CCC collaborate to receive data packets. Before accepting the data, the data's source must be validated. The data packet must be rejected if it originates from a malicious source. Authentication can be performed via a digital signature, digital certificate, MAC, or any other recognized identification method [7,8,12,18,19].
4. **Privacy:** The privacy of SG users is important during all the communications. If it is compromised, an adversary can observe an individual's electricity usage and infer sensitive information about his/her personal lifestyle [3,14–16,20]. It reveals information such as when he/she is not available at home or how much power the customer will use in the upcoming period.
5. **Anonymity:** If metering data need to be associated with a particular customer for billing or other purposes, they need to be anonymized before being released to other parties. From these data, the adversary may be unable to find the real identity of an SM [21].
6. **Differential privacy:** Differential privacy is a technique that ensures that the removal or addition of a single item in a statistical database has no effect on the outcome of any query on that database. Differential privacy is a measure of the trade-off between the accuracy of aggregated data and the likelihood of identifying individual data contributions within the aggregate. It is achieved by adding appropriate noise to metering data through a Laplace/Geometric distribution [9].

2.3. Performance Requirements

1. **Computational cost:** In the SG, the computational overhead is distributed across four stages: the individual users (SM), the aggregator (gateway), the CCC, and the TA [3]. Several modular operations are carried out during the encryption and decryption processes. The schemes based on public key infrastructure (PKI) are computationally intensive [6,8,9,16,17,22]. The computational cost also varies depending on how many times SM data are submitted, and aggregation takes place at the GW level.
2. **Communication overhead:** In the SG, data packets are shared between the SM, GW/FN, CCC, and TA. The cost of communication varies according to the number of messages/data packets shared and their size [23]. Security concerns must be addressed in order to avoid interfering with and interrupting data packets in transit or at rest [24]. Concerns about privacy and communication costs could be greatly reduced if the data aggregation process is used on consumption data [11].
3. **FT:** Any component have failed in the SG architecture needs to be found as quickly as is feasible and restored/repaired without causing a significant loss of service or other issues.
4. **Support temporal aggregation:** Temporal aggregation relates to the total electricity usage for a single smart meter in different time periods. It is required for billing purposes [13].
5. **Support random addition and removal of SMs:** SMs can be added or removed as per the requirement. If a new SM is installed, it must be configured before it can be included in the system for the purposes of capturing metering data and billing. An appropriate procedure must be in place to remove the configuration if any SM is damaged or removed. If necessary, an SM can also change areas due to relocation. When the SM is relocated, the appropriate gateway needs to be modified [8,25].
6. **Robustness:** In the SG, when the SM submits its data to the CCC, many cryptographic operations are required at various stages. The data aggregation technique must be robust in terms of security properties, storage costs, computational costs, and fault tolerance.
7. **Efficiency:** In the SG, there is much communication between SM components. Data transmission through those components must be secured using a variety of security techniques, such as public key cryptographic techniques and homomorphic functions. The use of security items at different stages must be efficient and use fewer resources in terms of storage and processing time.
8. **Storage cost:** Storage cost is related to storing the values of the various cryptographic operations generated during communication between different entities. Key length, signature, and hash values have a big impact on the Smart Grid because the SM has limited resources to store data [26].

As discussed above, the performance properties of state-of-the-art schemes indicate that the computational cost of a scheme is highly dependent on the cryptographic approach selected to support the security properties. A high number of cryptographic operations increase the computational cost of a scheme. It is observed that asymmetric-based cryptographic operations are more computationally resource hungry as compared to symmetric/non-asymmetric cryptography. However, the security features provided by asymmetric cryptography, especially homomorphic encryption schemes, support direct operations on encrypted data. The communication cost is dependent on the number of messages shared to transmit the SM data to the CCC. The concept of secure aggregation reduces overall communication, and the CCC is only required to decrypt the final aggregated value. The usage of fog nodes further reduces the overall communication, provides resources to perform various operations locally, and stores data for some [11]. FT is required to handle failed SMs' data. Some schemes, such as [7,23,27], use default or dummy values to accelerate CCC decryption. However, the results are not used for estimation purposes. For missing SMs, the scheme presented by [11] offers a way to store the most recently recorded value. In this case, the overall data usage is more accurate. The support for handling spatial

and temporal data also helps to improve SG billing operations [28]. SMs in the system are not always immutable; for example, the TA may occasionally add a new SM or revoke an old one. When a new SM is added, the TA will generate its private key. In the case of the SMPC scheme, the other group members need to be informed about the removal/addition of an SM [8].

3. Security Attacks

In this section, we provide a list of possible attacks that can be launched on SDA in SGs. These attacks are very important to understand the SDA in SGs. Some of these attacks are generic and can be launched on any distributed system. However, some of these attacks are specific to SG data aggregation only:

1. **Communication attack:** This attack is primarily carried out on the SG communication network (Wi-Fi/ZigBee) in order to disrupt or overload communication between the SM and FN/GW and to postpone decision-making activities at the CCC level [6,8,17,19,29–32]. An adversary can also observe the SG component's communication to read usage data [7,33].
2. **Differential attack:** In a differential privacy attack, the adversary can infer information from two adjacent datasets [7,12,34,35].
3. **Malware attack:** In this attack, undetectable malware is deployed at the CCC to steal [4,33,36,37] detailed electricity information [3,8,12,15,19,24,29–31,38], shut down CCC components, forge customer data, or produce false statistical data [4,10,24,30].
4. **Replay attack:** In this type of attack, an adversary can resend old packets to the CCC. Based on this wrong information, the CCC can make the wrong decisions regarding demand–response, forecasting, and billing [6,14,17].
5. **Man-in-the-middle (MITM) attack:** This is an active type of attack and typically occurs when a malicious user intercepts the communication between SG components. The prime objective is to observe the traffic flow to collect electricity usage preferences and infer customers' routines and other personal information [17,29].
6. **Dictionary attack:** In this attack, an adversary tries to guess the encryption keys by observing and comparing all packets travelling from the SM to the CCC [39].
7. **Collusive attack:** In the SG, the CCC and FN are considered honest-but-curious entities. There is a possibility that they may collude secretly to deceive some SMs. Therefore, protection is required so that if the FN and CC are colluding, they cannot obtain any data usage information about other SMs. A group of SMs can collude, drop their readings, and steal energy [40].
8. **Malicious data mining attack:** Anonymous data can be mined for information using the controllable property of the group signature in the SG, endangering the privacy of the user [41].
9. **Re-identification attack:** In this attack, an adversary observes the customer's physical presence, records the power usage indicators (which appliances are on or off), and compares these data with statistical information that is readily accessible to the public. These data are used to assess the energy usage level at each given moment [42].
10. **Privacy divulging:** An adversary may jeopardize residential users' privacy by listening in on communication data from residential users travelling towards the GW/FN and CCC [22].
11. **False data injection, fake, bad attack:** Intruders may attempt to compromise the SM and inject false information to impact the power grid's assessment status. In the SG, the CCC is treated as fully trusted, but in reality, it may share the user's consumption data with unauthorized and untrusted entities [43].
12. **Eclipse attack:** The eclipse attack is also related to peer-to-peer distributed networks. In this type of attack, the colluding gateways conspire to alter the construction of the aggregation trees by inducing the honest gateways to select them as their neighbors, to mediate most of the aggregation requests specified by the EEs.

13. **Denial-of-service (DoS) attack:** This targets the SM to halt its functionality and deprive it from submitting its data [3,6,8,17,33,34].
14. **Distributed denial-of-service (DoS) Attack:** This targets the AMI communication network to sabotage the communication flow between the wide area network (WAN) and neighborhood area network (NAN) [44].
15. **Data privacy attack:** Data privacy attack is related to observing or sharing customer data with malicious parties without their consent. Protection needs to be provided if external attackers, the CCC, and the FN/GW try to infer any knowledge about users from their usage data [43].

Some of the solutions to the above security attacks in the SG are discussed below. The author of the scheme in [7] added geometric distribution noise to the aggregatedGW to overcome differential privacy attacks. In the schemes in [23,40], a timestamp is used to handle replay attacks. In the scheme in [40], to avoid a colluding attack, the authors hid the actual identity of the sender SM and designated another SM to submit data on its behalf. The confidentiality of individual SM data is handled by encrypting customer data through the BGN cryptosystem and adding a random number to every data collection phase [11]. The authentication of the sender SM is handled through the MAC and ECDSA digital signature [11,23]. Protection against false data injection attacks is provided through a certificate or valid SM list [45,46].

4. Fault-Tolerant SDA Schemes in SGs

The FT schemes in SGs are divided into cryptographic and non-cryptographic categories. The crypto category is further divided into symmetric and asymmetric. The asymmetric category is further divided into lattice, homomorphic, and non-homomorphic schemes. The non-crypto schemes are divided into binary tree model, pairwise streaming, and coding theory schemes.

Cryptography Based FT SDA Schemes

The cryptographic schemes can be divided into symmetric and asymmetric schemes.

Symmetric Cryptography based FT SDA Schemes: Symmetric key cryptography, also known as private key cryptography, is the scheme in which a single, or master key, is used in the encryption and decryption processes. The transformation of plaintext to ciphertext utilizing the master key is known as encryption. In any case, changing ciphertext into plaintext is known as decryption, which is the reverse process of encryption. In symmetric cryptography, a single shared key needs to be kept secret at both ends to enable secure communication between a sender and receiver. Lu et al. [7] proposed a lightweight data aggregation scheme. The scheme's most notable feature is that it supports secure aggregation with FT. A session key, AES encryption, and a Laplace distribution are used to achieve privacy-preserving SDA. The authors added subtle strings during the data collection phase to deal with the faulty SM scenario. Sun et al. [22] proposed a fault-tolerant pairwise private stream aggregation scheme. The limitation of their scheme is that a faulty meter can be paired with another faulty meter due to random pairing. In Chan et al.'s [9] secure aggregation scheme, faulty SMs are handled through a binary tree based architecture. Their scheme is also secure against differential privacy attacks and supports dynamic SM addition and removal. In Wu et al.'s [17] scheme, the authors proposed a novel key management scheme that combines the symmetric key technique and the elliptic curve public key technique. The agents receive the symmetric key for internal communication from trusted anchors. If one of the trusted anchors is faulty, agents can be assigned to other less-loaded trust anchors for session key generation. Won et al. [10] proposed a proactive fault-tolerant aggregation algorithm based on future ciphertexts. During data submission, every SM divides its ciphertext into the current ciphertext and the future ciphertext. Future ciphertexts must be stored to ensure FT during SDA. However, it requires more storage on the aggregator end. A fog-enabled data aggregation (PPFA) scheme was proposed by Li et al. [27]. FNs periodically gather and aggregate data from the

corresponding SMs. The CCC aggregates the data gathered from all FNs. OTP is employed for encryption, while the PKC is configured for authentication. One disadvantage of the preceding approach is that keys of the same length as the plaintext must be created, as well as new keys each time. Furthermore, if any SMs fail, data aggregation will require an additional round of communication.

Asymmetric Cryptography based FT SDA Schemes: In asymmetric cryptography [38], two keys are used instead of a single key. It consists of a public key and a private key. The public key is available to everyone and serves only to encrypt data. The private key is only available to the key owner and is used to decrypt messages. Asymmetric cryptography provides several security features, such as message integrity, authentication, and non-repudiation. However, compared to symmetric cryptography, it is costly in terms of computation. Many schemes have been proposed based on asymmetric cryptography in the context of SDA in the SG. Asymmetric schemes can be divided into the subtypes homomorphic and non-homomorphic schemes.

Non-homomorphic schemes: Ni et al. [32] proposed a differentially private smart metering scheme (DiPrism) with FT and range-based filtering. Lifted-El Gamal encryption was used to aggregate SM data at the GW level. The range-based filtering method detects abnormal readings by comparing them to normal readings. All SMs' data are required to decrypt the aggregated data at the CCC level. When there are faulty SMs, the CCC works with the GW to obtain the aggregation values for the faulty SMs. Their scheme is secure against false data injection attacks by using the zero-knowledge range proof. In Li et al.'s [6] scheme, authentication is provided through a BLS-based signature during data aggregation. If one of the collectors is out of service, the standby collector can complete the authentication process through digital signatures and the minimum spanning tree (MST) without any further additional setup or configuration. Their scheme is resistant to replay and denial-of-service attacks. The disadvantage of this scheme is that it requires many computational resources.

Secure multiparty computation-based schemes: Secure multiparty computation (SMPC) is a branch of cryptography that enables distributed parties to jointly compute a function using their own inputs without disclosing their outputs. With the intention of enabling distributed computation without the requirement for a reliable third party, the initial work on SMPC started in 1970. In the 1980s, Yao published his first paper on SMPC [47]. Since then, SMPC has made significant strides in both theory and application [48]. Thoma et al. [49] proposed the SMPC-based homomorphic encryption scheme on the basis of individual SM load management. The utility can execute real-time demand management with specific consumers using SMC and a well-designed power plan without knowing the true value of each user's consumption data. Mustafa et al. [50] proposed an innovative solution based on SMPC that allows SG operators and suppliers to collect users' electricity metering data securely and privately. SMPC helps all recipients receive data related to transmission, distribution, and fee collections. The SPMC-based Shamir secret scheme is implemented in C++, and the BGW protocol [51,52] is used to support homomorphic encryption. A fog-enabled secure multiparty computation (SMPC) aggregation scheme in the SG was presented by Hayat et al. [40]. The scheme is robust against the collusion and false data injection (FDI) attacks during metering data collection. A collusion attack is managed through Shamir's enhanced secret scheme.

Homomorphic schemes: Homomorphic encryption (HE) is a method for performing operations on encrypted data while maintaining the confidentiality and integrity of the underlying data. There are two types of homomorphic encryption schemes: the fog-based and non-fog-based. Partial homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), and fully homomorphic encryption (FHE) schemes [53] are the three types of homomorphic encryption schemes.

Partial homomorphic encryption (PHE) schemes: The Paillier [8], Boneh–Goh–Nissim [14,54], and El Gamal encryption schemes are classical and state-of-the-art homomorphic encryption (HE) algorithms used in SG data aggregation. Bilinear mapping [6,17] is also

commonly used to generate and exchange keys for SG entities and during data aggregation.

Paillier encryption scheme: Chen et al. [8] proposed a privacy-preserving data aggregation scheme with FT in the SG. Their scheme supports customer data protections against an adversary that has the capability to compromise servers at the CCC. SM data are encrypted through Paillier encryption. For missing SMs, decryption activity can be completed by adjusting the default values provided by the TA. Zhitao et al. [33] proposed a fault-tolerant data aggregation scheme based on secret sharing. In their scheme, all SMs are split into different groups. SM IDs are masked through the anonymization process. Privacy is achieved through Paillier encryption by splitting secrets among SMs in a particular group. The malfunctioning SM is identified by comparing the group hash table value to the values of other groups. FT is achieved through a substitution mechanism. The proposed scheme is secure against collusion attacks. Jawurek et al. [38] proposed a protocol to calculate diverse statistics on SMs' data that supports FT and differential privacy. In the proposed scheme, the GW and TA are considered non-trustworthy. Paillier homomorphic encryption is used to encrypt SM data, and symmetric geometric distribution is used to ensure privacy. The scheme allows the aggregator to compute statistics based on available SMs' data, even if some SMs are faulty. Liu et al.'s [55] scheme supports statistical functions on encrypted data for IoT devices. The scheme is secure and fault-tolerant. FT is achieved through future data buffering mechanism.

El Gamal encryption scheme: Ni et al. [32] proposed a data aggregation scheme (DiPrism) for the SG that supports differential privacy, FT, and range-based filtering for AMI (advanced metering infrastructure). The metering data are encrypted through EI Gamal homomorphic encryption. Every SM includes a zero-knowledge (KW) proof during the encryption stage to ensure that readings are within a pre-defined range. Abnormal readings are filtered out based on the zero-knowledge proof. The Laplace distribution is used to add noise to achieve differential privacy.

Somewhat homomorphic encryption (SWHE): Somewhat homomorphic encryption (SWHE) is a homomorphic public key infrastructure (PKI). SWHE was the first of its kind to allow both multiplication and addition operations on encrypted data. Bao et al. [20] proposed a privacy-preserving data aggregation scheme with differential privacy and FT. Their scheme supports data aggregation activity in the presence of faulty SMs. The authors used the Boneh–Goh–Nissim (BGN) cryptosystem [56] to encrypt SM data and introduce noise via a Laplace distribution. To handle faulty SMs, a random value is added to the SM data. On the basis of this random value, the decryption activity is completed for working SMs. The scheme provides protection against the DP and eavesdropping attacks. Fu et al. [29] proposed a privacy-preserving and secure multidimensional aggregation scheme for the SG. Mykletun homomorphic encryption and the Boneh signature system are used in the proposed scheme to achieve privacy, integrity, authentication, and the identification of accidental errors. If some SMs have not submitted their data due to selective forwarding attacks or random errors, the GW will notify the CCC and TA of the list of faulty SMs. The CCC will calculate the hash sum of the faulty SMs and recover their data. Hayat et al. [11] presented a fog-enabled privacy-preserving SDA scheme with FT. The scheme provides protection against the FDI and replay attacks and ensures the confidentiality and authenticity of customer data. Techniques such as the modified BGN cryptosystem, homomorphic aggregation, and the elliptic curve digital signature algorithm (ECDSA) authentication mechanism are used to reduce the computational costs and communication overhead. Furthermore, the proposed scheme allows data aggregation to continue in the presence of faulty SMs.

Lattice-based schemes: Lattice-based cryptography is the alternative to the RSA and elliptic curve cryptography (ECC) public-key schemes. In Nth-degree truncated polynomial ring unit (NTRU) schemes, the encryption and decryption processes are simply polynomial arithmetic operations. Therefore, NTRU's implementation is efficient as compared to other asymmetric schemes. Asmaa et al. [57] proposed a lattice-based homomorphic privacy-preserving scheme in the SG. In this scheme, all appliances installed in one particular home

aggregate their data and submit them to the installed SM. The SM applies NTRU-based encryption to the aggregated data and submits them to the CCC. The proposed scheme supports customer privacy, integrity, and confidentiality. Furthermore, it is lightweight in terms of computational cost and communication overhead.

Table 1 gives an overview of existing FT aggregation schemes for the SG.

Table 1. Overview of fault-tolerance schemes in smart grids.

Technique Used	Attack Model	System Model	Strength	Weakness
Diluted geometric distribution, quad tree, key management centre (KMC) [15]	Malware, data pollution attacks	SM, CC, GW	Privacy, DP, FT, low compu. and comm. cost	Less effective, inefficient, and unreliable
Needham–Schroeder authentication protocol [17]	Replay, DDoS, MITM attack	SM, TA, GW	Scalability, FT	Unreliable, high comm. overhead and compu. cost
BLS signature aggregation, batch verification, signature amortization [6]	Replay, DDoS attack	SM, TTP, CA, GW	FT, availability, low comm. and compu. cost.	Less effective, inefficient, and unreliable
Paillier homomorphic cryptosystem, distributed key-managing authority [38]	Aggregator obliviousness, malicious data consumer	SM, aggregator	Exchangeable statistical functions, group key management, DP, FT	Only group signature verification facility
Binary tree,block aggregation, geometric distribution [9]	Colluding, data pollution attack	SM, aggregator, TA	FT, no peer-to-peer comm., dynamic leaver/joiner	Extra communication if tree expanded
Pairwise private stream aggregation scheme [22]	Eavesdrop, privacy-divulging attack	KMC, SM, CCC	FT, privacy	Extra comm. overhead
Coding theory, spread spectrum communication over CDMA [18]	DP, MITM, inference attack	SM, TA, GW, CDMA, CCC	Low comm. and compu. cost, high performance	Extra storage, unreliable
Homomorphic encryption, geometric distribution [19]	Privacy divulging, data attack	CCC, TA, GW, SM, CH	FT, DP privacy, low compu. and comm. cost	Slow verification process, configuration and maintenance issues
Paillier-based homomorphic encryption [12]	DP, malware, privacy divulging, data alteration attack	CC, TA, GW, KMC, SMs	Decentralized, FT, DP	High storage, comm., and compu cost
Paillier homomorphic encryption [8]	Data mining, DDoS, replay attack	SM, GW, CCC	Privacy, FT, comp. efficiency, DP	Less efficient, high compu. cost
BGN, Diffie–Hellmann key exchange protocol [20]	Internal, external, and differential attack	CC, TA, GW, SM	Privacy, FT, DP,low error, less comp. cost	High storage cost, configuration and maintenance issue
SMPC, homomorphic encryption [24]	MITM, data mining and differential attack	One aggregator model	Privacy-preserving	No secure channel, high comp. and compu. cost
HE signature scheme, El Gamal cryptosystem [30]	Chosen message attacks	CCC, SMs, GW	Less comm. and comp. cost, privacy, FT	Less efficient, high storage cost, unreliable
Modular addition symmetric key, digital certificates [31]	Curious aggregator, chosen message and chosen ciphertext attack	SM,Aggregator	Scalability, FT, DP, high accuracy	High bandwidth, extra storage requirement
El Gamal homomorphic encryption, 0-knowledge range proof, PKI cert [32]	DDoS,n data mining attacks	CCC,n GW,n SM,n TA	Privacy,n DP,n FT,n range-based filtering	Comm. overhead, compu. cost

Figure 3 shows the proposed taxonomy of fault-tolerant SDA schemes in the SG.

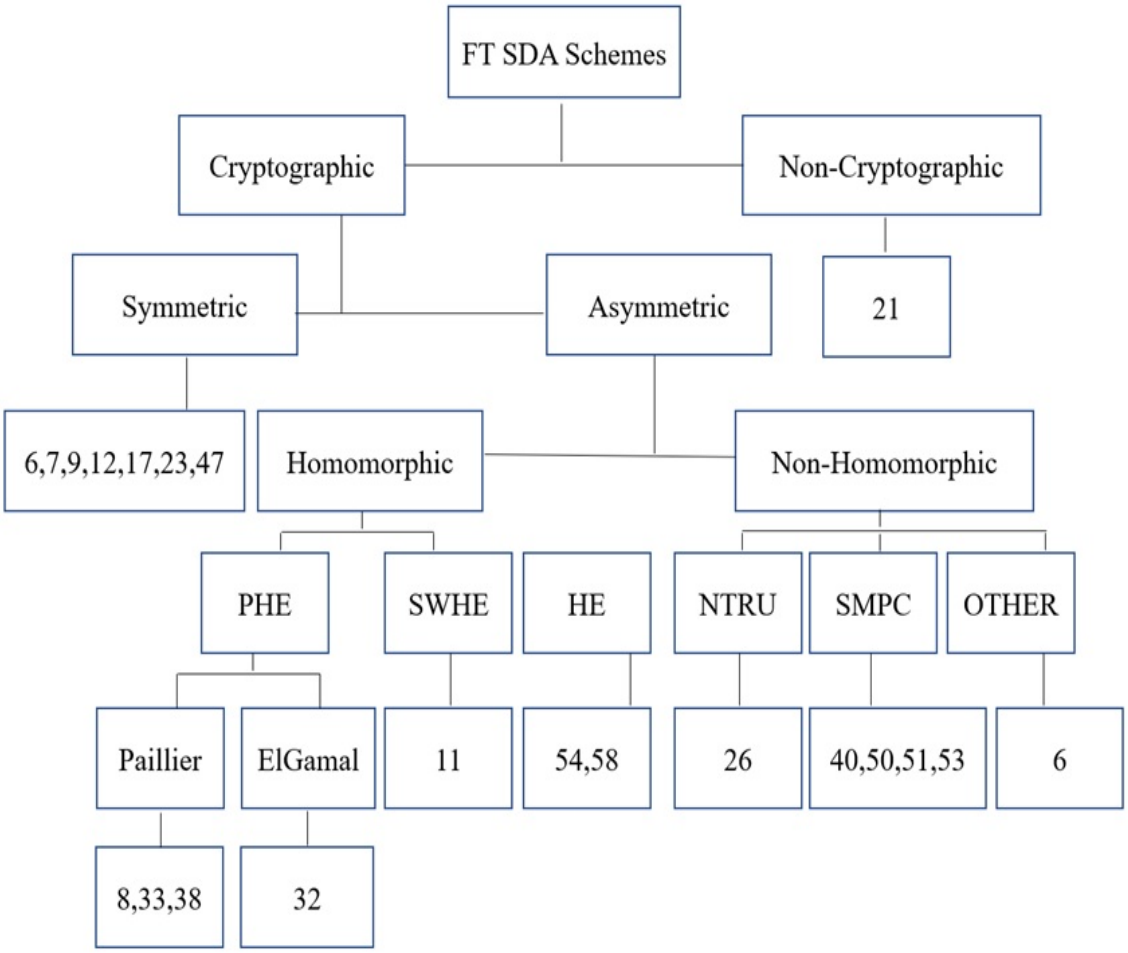

Figure 3. Taxonomy of FTSDA schemes in smart grids.

5. Comparative Analysis of SDA with FT Schemes

This section provides a brief comparison of the current state-of-the-art FTSDA in terms of security and performance properties.

5.1. Evaluation with Respect to Security Properties

In Table 2, trusted models of state-of-the-art schemes are evaluated based on their security properties. It can be observed from the existing literature on SGs that the dominant part of the introduced strategies satisfies the security prerequisites in SGs related to integrity, confidentiality, authenticity, privacy, robustness, efficiency, anonymity, adaptation to non-critical failure (FT), and differential privacy:

1. **Confidentiality:** The authors in [15] used a private stream aggregation (PSA) scheme to encrypt smart metering data. In the scheme in [17], ECC was used for key sharing between the data aggregator and collector. Scheme [22] uses pairwise private stream aggregation (PPSA) to encrypt smart metering data. In the scheme in [12], confidentiality was achieved through private key encryption. To support confidentiality, the authors of the schemes in [8,33] used Paillier encryption. In the schemes in [20,34], encryption is performed through the BGN cryptosystem. The authors of [30] used modular-based additive encryption to generate ciphertexts. In the scheme in [31], private stream aggregation is used to set up noisy encryption.
2. **Differential privacy:** To support DP, the scheme presented in [9] uses a randomized function to add noise to aggregated data before submitting them to the untrusted aggregator. The schemes in [7,9,34] use a geometric distribution to add noise at the GW level to achieve DP. The authors of the schemes in [19,20,30] added noise to SM

data through a Laplace distribution and supported DP. The authors in [12] used the binomial distribution to add noise to SM data.

3. **Data integrity:** The authors of the scheme in [15,19] achieved data integrity through the path signature method. For source authentication and data integrity, the scheme presented in [7] employs AES encryption.
4. **Authenticity:** The authors in [17] used the Needham–Schroeder protocol for SM and GW/FN authentication. The scheme in [6] uses the BLS signature scheme to authenticate SMs. A tree-based structure is used to verify each packet from an SM. In the scheme in [20], the Diffie–Hellmann key exchange protocol is used for authentication.
5. **Availability:** To achieve FT, the schemes mentioned in [15,19] use the quad tree. The authors in [7] introduced the auxiliary text to cater to faulty SM identification. In [12], the authors divided each SM into two groups of two members. If one of them fails, the decryption activity will fail. The working SM will be moved to another group where its member is working. The faulty SM will be taken care of accordingly. In the scheme in [8], if some servers at the CCC are compromised, the CCC can perform the decryption activity for the remaining $d - k$ servers. The scheme discussed in [20] is more robust against any rational number of malfunctioning SMs. Future ciphertext was used to handle FT in [30]. The scheme proposed in [34] supports both the CCC and SM failure scenarios. The scheme described in [33] provides FT via a substitution strategy.
6. **Protection against malware:** The scheme of [20] supports security against internal malware attacks. If the malware can infect the CCC, it can only reveal the aggregated value, but could not reveal individual users' data.
7. **Malicious data consumer:** Data consumers were deemed malicious in the scheme presented in [38]. Data security was achieved using the freshness key.

Table 2. Comparative analyses of security properties.

Ref.	SR1	SR2	SR3	SR4	SR5	SR6
[15]	✓	✗	✗	✓	✓	✗
[17]	✓	✗	✗	✓	✗	✗
[6]	✗	✗	✗	✓	✓	✗
[38]	✗	✓	✗	✗	✗	✓
[9]	✗	✓	✗	✗	✓	✗
[22]	✓	✓	✓	✓	✓	✗
[7]	✓	✓	✓	✓	✓	✗
[19]	✓	✓	✓	✓	✓	✗
[12]	✓	✓	✗	✗	✓	✗
[8]	✓	✓	✓	✓	✓	✗
[20]	✓	✓	✗	✗	✓	✓
[30]	✓	✓	✗	✗	✓	✓
[31]	✓	✓	✗	✗	✗	✗
[34]	✓	✓	✗	✗	✓	✗
[33]	✓	✗	✗	✗	✓	✗

SR1: confidentiality; SR2: differential privacy; SR3: data integrity; SR4: authenticity; SR5: availability; SR6: malware, malicious data consumer, data mining. ✗ indicates that security property is not fulfilled by this scheme, ✓indicates that security property is fulfilled by this scheme.

5.2. Evaluation with Respect to Performance Properties

In Table 3, trusted models of state-of-the-art schemes are evaluated based on their performance properties:

1. **Computational cost**: In existing state-of-the-art schemes in SGs, the computational cost is measured in terms of the number of cryptographic operations or the time required to perform the encryption and decryption activities. In the schemes in [15,19], encryption takes 0.6 seconds using an elliptic curve for the complete depth of the tree. In the scheme in [9], the encryption and decryption costs are approximately 9 s for 1000 SMs and $O(\sqrt{n})$, respectively. In the scheme in [9], for the best case, if there are

no failing meters, decryption will be performed in one round, and in the worst case, $w-1$ rounds will be required to perform decryption. In the scheme in [7], most of the computations are performed at the aggregator level. At the SM level, encryption requires 1 multiplication, 3 hash calculations, and 4 exponential operations. In the scheme in [12], cryptographic operations consist of 1 hash function calculation, 2 modular exponentiations, and a 1 multiplication operation. In the scheme in [34], encryption for a single user requires 2 modular exponential operations and 1 modular multiplication. In all schemes, The modular exponentiation operation takes most of the execution time compared to other operations.

2. **Communication overhead:** In the scheme in [6], the authors claimed that, through signature aggregation, the communication costs are reduced by 50% during message authentication. The authors of [9] claimed that the total communication cost of their scheme was O(nlogn). In the scheme in [22], the SM submits its encrypted data to the CCC in a single round of communication, and the total communication cost is $O(n)$. In the scheme in [7], communication is involved when data move from the SM to the cluster head, from the cluster head to the GW, and from the GW to the CCC. For one cluster, the communication cost is 1685 bits, and for the cluster to the GW, the overall communications cost is $1685w$ bits for w pairs of communication. In the scheme in [12], each SM has to send its encrypted data to the CCC in a single round of communication. The total communication in the SG is $O(n)$. In the scheme in [8], the communication overhead is divided into two parts: at the SM level and the overall communication. For user-level communication, if for Paillier cryptosystem, parameter k is considered as 512 bits, the size of the user report is 1024 bits for one-time report submission to the GW. For overall communication, the GW collects data from all n users, aggregates them into one single value, and submits them to the CCC. In the scheme in [31], with a cryptographic setup, the encryption operation consists of a hash function using SHA-256, 1 multiplication, and 2 modular exponentiation operations.
3. **FT:** The authors of the scheme in [15,19] supported detecting malfunctioning SMs by scanning the complete tree structure. The working SM blocks are separated from malfunctioning users' blocks. In the scheme in [16], the authors used a cloud model for ensuring redundancy in case of component failure during data processing. The authors of the scheme in [9] used a binary tree approach to find failed SMs. In the scheme in [22], FT is achieved through a pairing mechanism. If any SM fails to submit data, the remaining working SMS are moved to another working pair. In the scheme in [7], FT is achieved through the substitution of subtle strings. Each SM has to add this subtle string of text to its data. During decryption, SMs that have submitted this string are considered working SMs. The scheme presented in [8] supports FT through replica servers at the CCC. If one of the servers is compromised, the others can keep the setup working. In the scheme in [30], FT is achieved through the addition of future ciphertext to the current round of data. In this scheme, all SMs are paired. During data collection, the aggregator broadcasts the list of failed SMs who have not reported their data. In response to this, the working SM of a pair submits data on behalf of the faulty SM.
4. **Differential privacy:** In the schemes in [15,19], noise is added from a geometric distribution during data report generation by the user. The authors of the scheme in [38] claimed that they achieved differential privacy by introducing an O(1) error in the accuracy of the aggregation activity when there are failed SMs. The authors of the scheme in [9] used a geometric distribution to add noise to perturb the metering data. During the decryption process, if all noises cancel each other, the final estimate contains a noise of roughly O(logn). In the scheme in [7], to achieve differential privacy, noise is added from a geometric distribution to aggregated data at the gateway level. The authors calculated the root-mean-squared error (RMSE) for all the SMs and the malfunctioning SMs and claimed that their proposed scheme achieved better utility with lower errors. The binomial distribution is used in the scheme presented in [12]

to achieve differential privacy. Every SM perturbs its data with generated noise and encrypts them with its private key.

5. **Support dynamic meters' addition/removal:** The scheme presented in [9] supports dynamic joiners and leavers without rekeying operations. In the scheme in [12], when a new SM joins, it will contact the KMC. The KMC will place the SM in a specific group based on its properties and assign it a private key. The CCC is also updated to extend the decryption activity due to the addition of a new SM. In the scheme in [20], as only the TA knows the private key, when a new user joins, the TA generates its private key and updates the secret polynomial. Similarly, when an existing user leaves, its secret key is removed. In the scheme in [30], when the SM leaves, the GW needs to be informed. The GW will broadcast its ID to all SMs. The leaving decision will impact two types of SMs: the one that chose the leaving SM as its partner and the other who was chosen by the leaving SM as its partner.
6. **Storage cost:** In the scheme in [12], the number of keys stored depends on the number of SMs, the rounds of random grouping, and the size of each group. In the scheme in [30], the authors added future ciphertext in addition to current metering data to support FT. The authors claimed that the additional storage required to store future ciphertext is very small. However, for a small number of users, this can be ignored, but when the number of users increases to a large number, this brings large storage requirements to the grid. Patients in the scheme cited in S31 can visit mobile hospitals and are easily added to the system. Similarly, if a patient dies, his/her information can be removed.

Table 3. Comparative analyses of performance requirements.

Ref.	PR1	PR2	PR3	PR4	PR5	PR6	PR7
[15]	✓	✓	✗	✗	✗	✗	✗
[16]	✓	✓	✓	✓	✗	✗	✗
[17]	✓	✓	✓	✗	✗	✗	✗
[6]	✓	✓	✓	✗	✗	✗	✗
[38]	✗	✗	✓	✗	✗	✗	✗
[9]	✗	✗	✓	✓	✗	✗	✗
[22]	✓	✓	✓	✓	✗	✗	✗
[7]	✓	✓	✓	✓	✗	✗	✗
[19]	✓	✓	✓	✓	✗	✗	✗
[12]	✓	✓	✓	✓	✗	✗	✗
[8]	✓	✓	✓	✓	✗	✗	✗
[20]	✓	✓	✓	✗	✓	✓	✗
[24]	✓	✗	✓	✓	✗	✓	✓
[30]	✓	✓	✓	✗	✗	✗	✗
[31]	✗	✗	✗	✓	✗	✗	✗
[34]	✓	✓	✓	✓	✗	✗	✗

PR1: computational cost; PR2: communication overhead; PR3: fault tolerance; PR4: differential privacy; PR5: support temporal aggregation; PR6: support dynamic users; PR7: storage cost. ✗ indicates that performance requirement is not fulfilled by this scheme, ✓ indicates that performance requirement is fulfilled by this scheme.

6. Design Challenges and Future Trends

1. An efficient privacy-preserving aggregation protocol with enhanced error detection support should be designed [22,32,58]. Schemes shall be designed in such a way that they support the tracing of malfunctioning SMs. If malfunctioning SMs are present, they can be isolated in such a way that their absence has less impact on the data estimation at the CCC level. The impact of differential privacy noise addition should be lessened if large numbers of SMs are compromised or not participating in the aggregation protocol.
2. A scheme is required that can efficiently identify data forgery attacks and support the generation of provenance records to trace abnormal footprints [8,59,60]. The should be support for rich statistics [8,31]. A fault-tolerant solution in the SG that supports grace degradation if failures occur in SMs, controllers, or communication mediums should be designed.

3. The SG's internal infrastructure's security needs to be enhanced against physical or cyberattacks. Redundancy for critical components needs to be ensured [2].
4. A scheme that supports resistance against pollution and collusion attacks initiated by SG entities should be designed [3,15,19,61].
5. A dynamic pricing model in SGs should be designed and implemented [62]. Based on the usage data, customers can be categorized into different categories, such as gold, silver, and bronze. Incentives can be offered on the basis of usage data. Furthermore, customers can also generate electricity; therefore, a pricing model can be developed so that customers can sell their extra electricity in a competitive manner.
6. A secure aggregation scheme that minimizes communication overhead by minimizing message flow between SG entities should be designed [36,63,64].
7. Schemes based on advanced machine learning techniques to detect anomalies in the SM readings should be designed [65].

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Farhangi, H. The path of the Smart Grid. *IEEE Power Energy Mag.* **2009**, *8*, 18–28.
2. Lu, R.; Liang, X.; Li, X.; Lin, X.; Shen, X. EPPA: An efficient and privacy-preserving aggregation scheme for secure Smart Grid communications. *IEEE Trans. Parallel Distrib. Syst.* **2012**, *23*, 1621–1631.
3. Li, X.; Liang, X.; Lu, R.; Shen, X.; Lin, X.; Zhu, H. Securing Smart Grid: Cyber attacks, countermeasures, and challenges. *IEEE Commun. Mag.* **2012**, *50*, 38–45.
4. Wang, W.; Lu, Z. Cyber security in the Smart Grid: Survey and challenges. *Comput. Netw.* **2013**, *57*, 1344–1371.
5. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J.; Shu, L. A systematic review of data protection and privacy preservation schemes for Smart Grid communications. *Sustain. Cities Soc.* **2018**, *38*, 806–835.
6. Li, D.; Aung, Z.; Williams, J.R.; Sanchez, A. Efficient authentication scheme for data aggregation in Smart Grid with fault tolerance and fault diagnosis. In Proceedings of the 2012 IEEE PES Innovative Smart Grid Technologies (ISGT), Washington, DC, USA, 16–20 January 2012; pp. 1–8.
7. Bao, H.; Lu, R. A lightweight data aggregation scheme achieving privacy preservation and data integrity with differential privacy and fault tolerance. *Peer -Peer Netw. Appl.* **2017**, *10*, 106–121.
8. Chen, L.; Lu, R.; Cao, Z. PDAFT: A privacy-preserving data aggregation scheme with fault tolerance for Smart Grid communications. *-Peer -Peer Netw. Appl.* **2015**, *8*, 1122–1132.
9. Chan, T.H.H.; Shi, E.; Song, D. Privacy-preserving stream aggregation with fault tolerance. In *Proceedings of the International Conference on Financial Cryptography and Data Security*; Springer: Cham, Switzerland, 2012; pp. 200–214.
10. Won, J.; Ma, C.Y.; Yau, D.K.; Rao, N.S. Privacy-assured aggregation protocol for smart metering: A proactive fault-tolerant approach. *IEEE/ACM Trans. Netw.* **2015**, *24*, 1661–1674.
11. Khan, H.M.; Khan, A.; Jabeen, F.; Rahman, A.U. Privacy preserving data aggregation with fault tolerance in fog-enabled Smart Grids. *Sustain. Cities Soc.* **2021**, *64*, 102522.
12. Shi, Z.; Sun, R.; Lu, R.; Chen, L.; Chen, J.; Shen, X.S. Diverse grouping-based aggregation protocol with error detection for Smart Grid communications. *IEEE Trans. Smart Grid* **2015**, *6*, 2856–2868.
13. Dwork, C. Differential privacy: A survey of results. In *Proceedings of the International Conference on Theory and Applications of Models of Computation*; Springer: Cham, Switzerland, 2008; pp. 1–19.
14. Sridhar, S.; Hahn, A.; Govindarasu, M. Cyber–physical system security for the electric power grid. *Proc. IEEE* **2011**, *100*, 210–224.
15. Lu, M.; Shi, Z.; Lu, R.; Sun, R.; Shen, X.S. PPPA: A practical privacy-preserving aggregation scheme for smart grid communications. In Proceedings of the 2013 IEEE/CIC International Conference on Communications in China (ICCC), Xi'an, China 12–14 August 2013; pp. 692–697.
16. Rusitschka, S.; Eger, K.; Gerdes, C. Smart grid data cloud: A model for utilizing cloud computing in the Smart Grid domain. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 483–488.
17. Wu, D.; Zhou, C. Fault-tolerant and scalable key management for Smart Grid. *IEEE Trans. Smart Grid* **2011**, *2*, 375–381.
18. Alamatsaz, N.; Boustani, A.; Jadliwala, M.; Namboodiri, V. Agsec: Secure and efficient cdma-based aggregation for smart metering systems. In Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 10–13 January 2014; pp. 489–494.
19. Bao, H.; Lu, R. Ddpft: Secure data aggregation scheme with differential privacy and fault tolerance. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7240–7245.

20. Bao, H.; Lu, R. A new differentially private data aggregation with fault tolerance for Smart Grid communications. *IEEE Internet Things J.* **2015**, *2*, 248–258.
21. Yang, L.; Li, F. Detecting false data injection in Smart Grid in-network aggregation. In Proceedings of the 2013 IEEE International Conference on Smart Grid Communications (SmartGridComm), Vancouver, Canada, 21–24 October 2013; pp. 408–413.
22. Sun, R.; Shi, Z.; Lu, R.; Lu, M.; Shen, X. APED: An efficient aggregation protocol with error detection for Smart Grid communications. In Proceedings of the 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 9–13 December 2013; pp. 432–437.
23. Saleem, A.; Khan, A.; Malik, S.U.R.; Pervaiz, H.; Malik, H.; Alam, M.; Jindal, A. FESDA: Fog-enabled secure data aggregation in Smart Grid IoT network. *IEEE Internet Things J.* **2019**, *7*, 6132–6142.
24. Jung, T.; Li, X.Y.; Wan, M. Collusion-tolerable privacy-preserving sum and product calculation without secure channel. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 45–57.
25. Nitaj, A. Cryptanalysis of NTRU with Two Public Keys. Cryptology ePrint Archive 2011. Available online: https://eprint.iacr.org/2011/477 (accessed on 22 October 2022).
26. Saxena, N.; Choi, B.J. State of the art authentication, access control, and secure integration in Smart Grid. *Energies* **2015**, *8*, 11883–11915.
27. Lyu, L.; Nandakumar, K.; Rubinstein, B.; Jin, J.; Bedo, J.; Palaniswami, M. PPFA: Privacy preserving fog-enabled aggregation in Smart Grid. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3733–3744.
28. Erkin, Z.; Tsudik, G. Private computation of spatial and temporal power consumption with smart meters. In *Proceedings of the International Conference on Applied Cryptography and Network Security*; Springer: Cham, Switzerland, 2012; pp. 561–577.
29. Fu, S.; Ma, J.; Li, H.; Jiang, Q. A robust and privacy-preserving aggregation scheme for secure smart grid communications in digital communities. *Secur. Commun. Netw.* **2016**, *9*, 2779–2788.
30. Won, J.; Ma, C.Y.; Yau, D.K.; Rao, N.S. Proactive fault-tolerant aggregation protocol for privacy-assured smart metering. In Proceedings of the IEEE INFOCOM 2014-IEEE Conference on Computer Communications, Toronto, Canada 27 April–2 May 2014; pp. 2804–2812.
31. Shi, R.; Chow, R.; Chan, T.H.H. Privacy-Preserving Aggregation of Time-Series Data. European Patent Office EP2485430B1, 14 September 2016.
32. Ni, J.; Zhang, K.; Alharbi, K.; Lin, X.; Zhang, N.; Shen, X.S. Differentially private smart metering with fault tolerance and range-based filtering. *IEEE Trans. Smart Grid* **2017**, *8*, 2483–2493.
33. Guan, Z.; Si, G.; Du, X.; Liu, P. Protecting User Privacy Based on Secret Sharing with Error Tolerance for Big Data in Smart Grid. *arXiv* **2018**, arXiv:1811.06918.
34. Han, S.; Zhao, S.; Li, Q.; Ju, C.H.; Zhou, W. PPM-HDA: Privacy-preserving and multifunctional health data aggregation with fault tolerance. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 1940–1955.
35. Ferrag, M.A.; Maglaras, L.A.; Janicke, H.; Jiang, J. A survey on privacy-preserving schemes for Smart Grid communications. *arXiv* **2016**, arXiv:1611.07722.
36. Hoepman, J.H. Privacy friendly aggregation of smart meter readings, even when meters crash. In Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, Pittsburgh, PA, USA, 21 April 2017; pp. 3–7.
37. Chen, J.; Ma, H.; Zhao, D. Private data aggregation with integrity assurance and fault tolerance for mobile crowd-sensing. *Wirel. Netw.* **2017**, *23*, 131–144.
38. Jawurek, M.; Kerschbaum, F. Fault-tolerant privacy-preserving statistics. In *Proceedings of the International Symposium on Privacy Enhancing Technologies Symposium*; Springer: Cham, Switzerland, 2012; pp. 221–238.
39. Bayat, M.; Atashgah, M.B.; Aref, M.R. A secure and efficient chaotic maps based authenticated key-exchange protocol for Smart Grid. *Wirel. Pers. Commun.* **2017**, *97*, 2551–2579.
40. Khan, H.M.; Khan, A.; Jabeen, F.; Anjum, A.; Jeon, G. Fog-enabled secure multiparty computation based aggregation scheme in Smart Grid. *Comput. Electr. Eng.* **2021**, *94*, 107358.
41. Shen, H.; Liu, Y.; Xia, Z.; Zhang, M. An efficient aggregation scheme resisting on malicious data mining attacks for Smart Grid. *Inf. Sci.* **2020**, *526*, 289–300.
42. Yang, L.; Xue, H.; Li, F. Privacy-preserving data sharing in Smart Grid systems. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 878–883.
43. Dong, X.; Zhou, J.; Alharbi, K.; Lin, X.; Cao, Z. An El Gamal-based efficient and privacy-preserving data aggregation scheme for Smart Grid. In Proceedings of the 2014 IEEE Global Communications Conference, Istanbul, Turkey, 6–9 May 2014; pp. 4720–4725.
44. Mendel, J. Smart grid cyber security challenges: Overview and classification. *e-Mentor* **2017**, pp. 55–66. http://dx.doi.org/10.15219/em68.1282.
45. Li, B.; Lu, R.; Xiao, G.; Su, Z.; Ghorbani, A. PAMA: A proactive approach to mitigate false data injection attacks in Smart Grids. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
46. Sun, A.; Wu, A.; Zheng, X.; Ren, F. Efficient and privacy-preserving certificateless data aggregation in Internet of things–enabled Smart Grid. *Int. J. Distrib. Sens. Networks* **2019**, *15*, 1550147719842062.
47. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), Chicago, IL, USA, 3–5 November 1982; pp. 160–164.

48. Zhao, C.; Zhao, S.; Zhao, M.; Chen, Z.; Gao, C.Z.; Li, H.; Tan, Y.a. Secure multiparty computation: Theory, practice and applications. *Inf. Sci.* **2019**, *476*, 357–372.
49. Thoma, C.; Cui, T.; Franchetti, F. Secure multiparty computation based privacy preserving smart metering system. In Proceedings of the 2012 North American Power Symposium (NAPS), Champaign, IL, USA, 9–11 September 2012; pp. 1–6.
50. Mustafa, M.A.; Cleemput, S.; Aly, A.; Abidin, A. An MPC-based protocol for secure and privacy-preserving smart metering. In Proceedings of the 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), Torino, Italy, 26–29 September 2017; pp. 1–6.
51. Ben-Or, M.; Goldwasser, S.; Wigderson, A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*; ACM: New York, NY, USA, 2019; pp. 351–371.
52. Mustafa, M.A.; Cleemput, S.; Aly, A.; Abidin, A. A secure and privacy-preserving protocol for smart metering operational data collection. *IEEE Trans. Smart Grid* **2019**, *10*, 6481–6490.
53. Tonyali, S.; Akkaya, K.; Saputro, N.; Uluagac, A.S.; Nojoumian, M. Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled smart metering systems. *Future Gener. Comput. Syst.* **2018**, *78*, 547–557.
54. Ács, G.; Castelluccia, C. I have a dream!(differentially private smart metering). In *Proceedings of the International Workshop on Information Hiding*; Springer: Cham, Switzerland, 2011; pp. 118–132.
55. Liu, H.; Chen, J.; Lin, L.; Ye, A.; Huang, C. An efficient and privacy-preserving data aggregation scheme supporting arbitrary statistical functions in IoT. *China Commun.* **2022**, *19*, 91–104.
56. Boneh, D.; Goh, E.J.; Nissim, K. Evaluating 2-DNF formulas on ciphertexts. In Proceedings of the Theory of Cryptography Conference; Springer: Cham, Switzerland, 2005; pp. 325–341.
57. Abdallah, A.; Shen, X.S. A lightweight lattice-based homomorphic privacy-preserving data aggregation scheme for Smart Grid. *IEEE Trans. Smart Grid* **2016**, *9*, 396–405.
58. Ni, J.; Zhang, K.; Lin, X.; Shen, X.S. EDAT: Efficient data aggregation without TTP for privacy-assured smart metering. In Proceedings of the 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 22–27 May 2016; pp. 1–6.
59. Li, F.; Luo, B.; Liu, P. Secure information aggregation for Smart Grids using homomorphic encryption. In Proceedings of the 2010 First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, USA, 4–6 October 2010; pp. 327–332.
60. Cho, S.; Li, H.; Choi, B.J. PALDA: Efficient privacy-preserving authentication for lossless data aggregation in Smart Grids. In Proceedings of the 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), Venice, Italy, 3–6 November 2014; pp. 914–919.
61. Bakondi, B.G.; Peter, A.; Everts, M.; Hartel, P.; Jonker, W. Publicly verifiable private aggregation of time-series data. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security, Toulouse, France, 24–28 August 2015; pp. 50–59.
62. Li, S.; Xue, K.; Yang, Q.; Hong, P. PPMA: Privacy-preserving multisubset data aggregation in Smart Grid. *IEEE Trans. Ind. Informatics* **2017**, *14*, 462–471.
63. Chen, L.; Lu, R.; Cao, Z.; AlHarbi, K.; Lin, X. MuDA: Multifunctional data aggregation in privacy-preserving smart grid communications. *Peer -Peer Netw. Appl.* **2015**, *8*, 777–792.
64. Borges, F.; Demirel, D.; Böck, L.; Buchmann, J.; Mühlhäuser, M. A privacy-enhancing protocol that provides in-network data aggregation and verifiable smart meter billing. In Proceedings of the 2014 IEEE Symposium on Computers and Communications (ISCC), Madeira, Portugal, 23–26 June 2014, pp. 1–6.
65. Keoh, S.L.; Tang, Z. Towards secure end-to-end data aggregation in AMI through delayed-integrity-verification. In Proceedings of the 2014 10th International Conference on Information Assurance and Security, Okinawa, Japan, 28–30 November 2014; pp. 6–11.