AN EFFICIENT PRIVACY PRESERVING MULTIPLE DATA AGGREGATION SCHEME WITHOUT TRUSTED AUTHORITY FOR FOG BASED SMART GRID

[1] K. UDAY KRUSHNA,[2] J. PRASHANTH,[3] P. SHASHANK,[4] V.SAI SRAVAN REDDY,[5] Mrs. A. NANDINI SREE

[1234] Students, [5] Assistant Professor

Department Of Computer Science and Design

Teegala Krishna Reddy Engineering College, Meerpet, Balapur, Hyderabad-500097

ABSTRACT

With the increasingly powerful and extensive deployment of edge devices, edge/fog computing enables customers to manage and analyze data locally, and extends computing power and data analysis applications to network edges. Meanwhile, as the next generation of the power grid, the smart grid can achieve the goal of efficiency, economy, security, reliability, use safety and environmental friendliness for the power grid. However, privacy and secure issues in fog-based smart grid communications are challenging. Without proper protection, customers' privacy will be readily violated. This paper presents a smart and practical Privacy-preserving Data Aggregation (PDA) scheme with smart pricing and packing method for fog-based smart grids, which achieves diversified tariffs, multifunctional statistics and efficiency. Especially, we first propose a smart PDA scheme with Smart Pricing (PDA-SP). With PDA-SP, the Control Center (CC) can compute more complex and higher-order aggregation statistics to provide various services, provide diversiform pricing strategies and choose a double-winning strategy. Subsequently, we put forward a practical PDA scheme with Packing Method (PDA-PM), which is able to reduce the size of encrypted data and improve performance in performing various secure computations. Moreover, we extend our original packing method and present a more useful packing method, which can handle general vectors with large entries. The security analysis shows that our proposed scheme is secure against many threats. The performance evaluation reveals that the computation and communication overheads of our proposed scheme are effectively reduced by employing the Somewhat Homomorphic Encryption (SHE), and our packing method can further significantly reduce these overheads.

I. INTRODUCTION

FOG/EDGE computing extends from cloud computing and has been booming in recent years. Fog/edge computing enables customers to realize computation, communication and storage locally, and extends functions of cloud computing to network edges. In the big data era, users have higher expectations for service quality and network performance. Traditional cloud computing has a significant shortage of storage capacity and computing power while handling a large number of user queries and reports. Therefore, it is beneficial to transfer some of the cloud's functionalities to the fog node.

Fog/edge computing has the advantages of fast response, low delay, fog volatility, large position perception, and enhanced safety and reliability in comparison with cloud computing. The above fascinating advantages have contributed to the appearance of fog-based smart grids and other Industrial Internet of Things. As the next generation of the power grid, the smart grid can achieve the goal of efficiency, economy, security, reliability, use safety and environmental friendliness for the power grid. The fog node enables the utility company to provide various services by the service query and command control between customers and the CC, such as adjusting the price of electricity, obtaining the overall power consumption, charging the customer for electricity and providing additional power according to customers' requirements. However, it's very challenging for privacy and security in the fog-based smart grid communication. Because electricity usage data involve customers' energy usage patterns, which are closely related to their private lives, improper handling of these data may cause the disclosure of customers' privacy.

In addition, diversified tariffs, multifunctional statistics and efficiency also should be taken into careful consideration. First, traditional tariffs are usually using the fixed pricing to calculate customers' electricity bills and considering a limited pricing strategy. With the development of fog-based smart grids and power grids, these traditional tariffs are insufficient to meet the requirements of fair pricing and intelligent electronic devices. Therefore, a diversiform PDA scheme (which can achieve diversified tariffs) is urgent to be put forward. Second, with the ever-increasing demands from power consumers, for providing various services, the CC needs to calculate more complex and higher-order statistic functions. However, many previous works are only supporting one-depth homomorphic multiplication, which are not powerful enough. Therefore, a multifunctional PDA scheme (which supports the CC to calculate statistic functions whose degree is larger than 2) is critical to be proposed. Third, the CC, fog nodes and customers should spend as low as possible on computations and communications. However, the bilinear pairing technology is employed in a lot of previous works, which poses a heavy burden on the CC and fog nodes. It is urgent to present an efficient PDA scheme for fog-based smart grids.

1.1 Motivation

With the rapid advancement and widespread deployment of fog/edge computing technologies, there is a pressing need to manage and analyze data closer to users, especially in critical infrastructures like smart grids. Smart grids promise efficiency, security, reliability, and environmental friendliness, but they also introduce significant challenges in terms of privacy and secure communications. Traditional approaches, with fixed pricing models and limited computational capabilities, are no longer sufficient to meet the evolving demands for diversified tariffs, multifunctional statistics, and operational efficiency. Moreover, the sensitive nature of electricity consumption data calls for robust privacy-preserving mechanisms. Therefore, the motivation behind this project is to develop a smart, practical, and efficient Privacy-preserving Data Aggregation (PDA) scheme with advanced smart pricing and packing methods for fog-based smart grids, ensuring secure, scalable, and dynamic service delivery while protecting user privacy.

1.2 Problem Statement

Despite the growing adoption of fog-based smart grids, current systems face significant limitations in handling secure and efficient data aggregation while ensuring user privacy. Traditional pricing models lack flexibility, and most existing Privacy-preserving Data Aggregation (PDA) schemes support only simple statistical functions with high computation and communication overhead due to reliance on bilinear pairing technologies. These issues hinder the ability of control centers to perform complex analysis, offer dynamic pricing strategies, and respond to increasing consumer demands. Therefore, there is a critical need for a multifunctional, efficient, and privacy-preserving PDA scheme that enables diversified tariffs, supports higher-order statistical computations, and minimizes resource usage in fog-based smart grid environments.

1.3 Scope and Objective

The scope of this project is to design and implement a smart and practical Privacy-preserving Data Aggregation (PDA) scheme tailored for fog-based smart grids, addressing the challenges of data security, efficiency, and dynamic pricing. The objective is to develop a system that enables secure and efficient data aggregation through the use of Somewhat Homomorphic Encryption (SHE) and an innovative packing method, allowing the control center to compute complex, higher-order statistical functions. Additionally, the scheme introduces smart pricing strategies that promote fair billing and influence user energy consumption behavior, all while significantly reducing computation and communication overhead to ensure scalability and real-world applicability.

II. LITERATURE SURVEY

Our scheme is to achieve multifunctional and efficient PDA, which is similar to a lot of related works published in recent literatures. Generally, there are two groups of PDA schemes: statistic-oriented PDA which is designed to perform various statistical analyses on remote sensing data, and efficiency- oriented PDA which focuses on raising efficiency.

Concerning statistic-oriented PDA, Shi et al. [11] present a PDA scheme, which uses data mixing and slicing to support max/min and additive aggregations. Subsequently, Li et al. [12] provide an efficient sum and min aggregation over ciphertexts by employing additive homomorphic encryption and key management. For ensuring data integrity and user privacy, Zhang et al.

[13] come up with a new method to verify PDA, which achieves multifunctional additive and nonadditive aggregations, i.e. sum, variance, max/min, median, percentile, histogram and count. In [14], Chen et al. present a PDA scheme with diversiform statistical functions. In addition to average aggregation, their scheme also realizes differential privacy of one-way ANOVA and variance aggregations. In order to achieve non-additive aggregation and differential privacy, Han et al. [15] propose a scheme, which realizes multifunctional additive and non-additive aggregation simultaneously. Sun et al. [16] present a scheme named Pri Stream, which enables privacy-preserving and communication-efficient distributed stream monitoring of thresholder percentile aggregates. A privacy-aware data aggregation and task allocation scheme is put forward by Wu et al. [17]. Their scheme achieves basic statistics (i.e. sum, variance and min) and efficient data update in a privacy-preserving way.

Concerning efficiency-oriented PDA, traditional schemes are mostly based on homomorphic encryption technology. Traditional homomorphic encryption scheme allows meaningful calculation over ciphertexts and improves computational efficiency, it can be categorized into three types: 1) Paillier based PDA schemes [18]– [23], which employ Paillier encryption system [24] to provide either adding or multiplying encrypted ciphertexts, but not both operations at the same time. 2) BGN-based PDA schemes [14], [15], [25], [26], which use BGN encryption system [27] to construct a scheme that can perform addition and multiplication simultaneously. These schemes handle any number of additions and just one multiplication. 3) The other pairing-based PDA schemes [28]– [32], which utilize bilinear pairing and homomorphic encryption to achieve efficient PDA. However, these pairing based schemes can perform arbitrarily number of additions, but also only allow one-depth homomorphic multiplication, which are not really expanded. In 2009, Gentry [33] makes an important breakthrough. He presented the Fully Homomorphic Encryption (FHE) scheme for the first time, which is based on the problems of hard lattice and handles any number of additions and multiplications, so that it enables to calculate arbitrary statistics securely. Unfortunately, this scheme is too complicated to be used in practice. Interestingly, some FHE schemes are associated with more practical SHE schemes that support any number of additions but allow for a limited number of multiplications. In this paper, we will use SHE to achieve privacy-preserving encryption and decryption. More importantly, we note that the above researches have two crucial flaws. On one hand, in the statistic-oriented PDA schemes, most works are utilizing bilinear pairing and homomorphic encryption to realize multifunctional addition and non-addition aggregations. However, these works are only supporting one-depth homomorphic multiplication over ciphertexts, which means that the aggregator cannot aggregate the users' data in a privacy-preserving way for any given statistic function whose degree is larger than 2. On the other hand, in the efficiency-oriented PDA schemes, a lot of works.

EXISTING SYSTEM

Traditional tariffs are usually using the fixed pricing to calculate customers' electricity bills and considering limited pricing strategies. With the development of fog-based smart grids and power grids, these traditional tariffs are insufficient to meet the requirements of fair pricing and intelligent electronic devices. Therefore, a diversiform PDA scheme (which can achieve diversified tariffs) is urgent to be put forward. Second, with the ever-increasing demands from power consumers, for providing various services, the CC needs to calculate more complex and higher-order statistic functions. However, many previous works are only supporting one-depth homomorphic multiplication, which are not powerful enough. Therefore, a multifunctional PDA scheme (which supports the CC to calculate statistic functions whose degree is larger than 2) is critical to be proposed. Third, the CC, fog nodes and customers should spend as low as possible on computations and communications. However, the bilinear pairing technology is employed in a lot of previous works, which poses a heavy burden on the CC and fog nodes. It is urgent to present an efficient PDA scheme for fog-based smart grids.

PROPOSED SYSTEM

For achieving diversified tariffs, multifunctional statistics and efficiency, in this paper, we propose a smart and practical PDA scheme for fog-based smart grids with smart pricing and packing method. We conclude our contributions as follows:

Almost all the previous works are only taking fixed pricing into consideration or the alternative pricing strategies are limited, and traditional tariffs are insufficient to meet the requirements of fair pricing. In response to such needs, we introduce smart pricing into the fog based smart grid. Thanks to its peculiar features, the CC can provide diversiform pricing strategies, and indirectly guide customers to dynamically adjust their energy usage patterns based on changes in electricity prices. In addition, our proposed scheme also can perform one-way analysis of variance (ANOVA) to evaluate whether these pricing strategies have an impact on customers' electricity usage behavior, and choose a double-winning strategy.

As the CC may need to compute more complex and higher-order statistic functions to provide various services, we introduce a multifunctional PDA scheme, which not only supports multifunctional additive and non-additive aggregations, but also supports the CC to calculate statistic functions whose degree is larger than 2. In addition, we also present two types of min aggregation protocols for fog-based smart grids, and compare the computation and communication overheads of them.

For reducing the size of encrypted data and improving performance when performing various secure computations, we come up with a new packing method for our PDA scheme. Our new packing method provides four types of packed ciphertexts for vectors, which is different from the message encoding technique presented by Lauter, Naehrig and Vaikuntanathan, and makes our proposed scheme efficient in both ciphertext size and performance. In addition, we present a more useful packing method, which can handle general vectors with large entries.

We introduce SHE into the fog-based smart grid, compared with previous works that utilizing bilinear pairing and homomorphic encryption, the computation and communication overheads are effectively reduced. Furthermore, the performance evaluation reveals that our packing method can further significantly reduce these overheads, which means our scheme is lightweight and efficient.

III. MODULE DESCRIPTION

The fog-based smart grid system consists of a trusted authority (TA), a utility company and a CC, some substations and some fog nodes, some communities and each community contain a number of customers, which are equipped with smart meters. Figure 1 describes our system model.

- **Trusted Authority:** The TA takes charge of entity registration and it is a powerful third party. It will go off-line after booting the whole system.
- **Control Center and Utility Company:** The CC collects, processes and analyzes real-time smart meter data and issues grid commands to smart meters and substations to provide customers with reliable grid services. The utility company is responsible for electrical power generation, storage and distribution.
- **Fog Node and Substation:** The flows of information between customers' smart meters and the CC, which contain smart meter readings, requests and commands, are preserved, processed and forwarded by the fog node. The substation waits for the utility company's commands and stores the electricity and transmits the electricity power to customers' houses.

Customer: Each customer's house with a smart meter, which gathers electricity usage data in real-time, relays these data and requests of grid service to the CC.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE

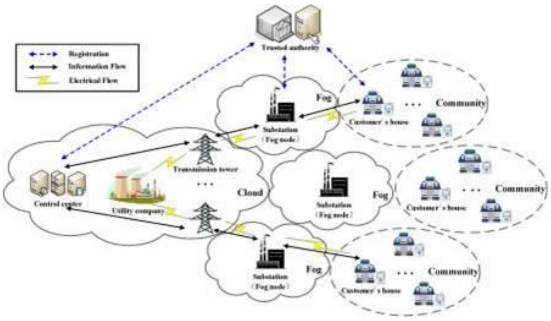
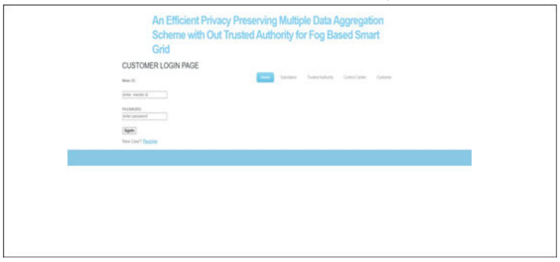


Fig. System Architecture

V. OUTPUT SCREENS

Smart and Practical Privacy-preserving Data Aggregation for Fog-based Smart Grids

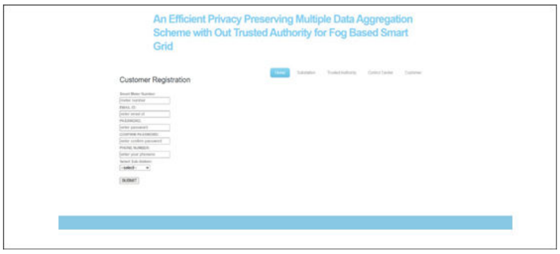
FIGURE: Home Page


An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

CUSTOMER LOGIN PAGE

Meter ID:
enter meter id
PASSWORD:
enter password

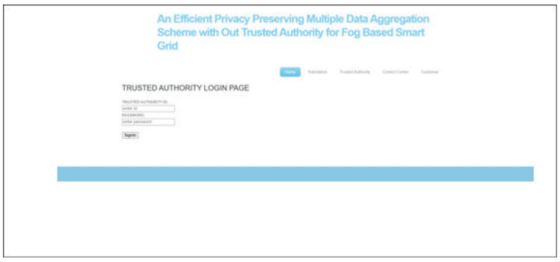
FIGURE: Customer Page


An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

Customer Registration

Smart Meter Number:
meter number
EMAIL ID:
enter email id
PASSWORD:
enter password
CONFIRM PASSWORD:
enter confirm password
PHONE NUMBER:
enter your phoneno
Select Sub-Station:
--select--

FIGURE: Customer Registration Page


An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

TRUSTED AUTHORITY LOGIN PAGE

TRUSTED AUTHORITY ID:
enter id
PASSWORD:
enter password

FIGURE: Trusted Authority Login Page

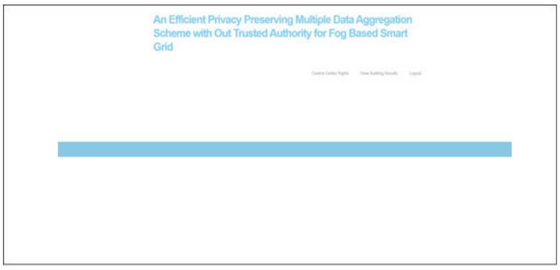
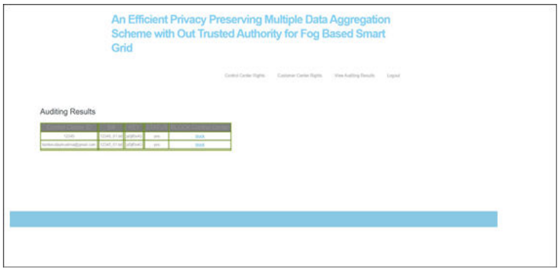

An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

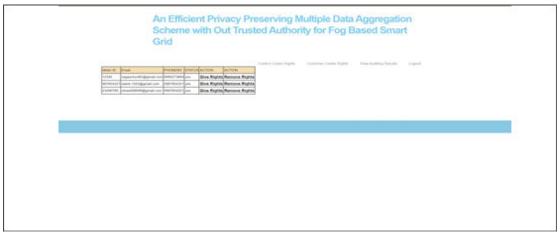
FIGURE: Trusted Authority Home Page


An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

Auditing Results

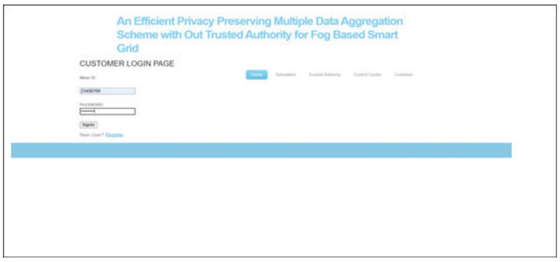
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
12345	12345_01.txt	[illegible]	yes	block
[illegible]@gmail.com	12345_01.txt	[illegible]	yes	block

FIGURE: Viewing Auditing Result Page



An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

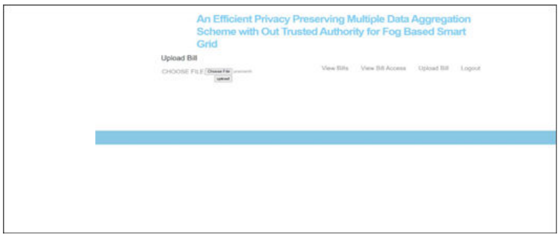
FIGURE: Giving Customer Control Rights Page



An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

CUSTOMER LOGIN PAGE

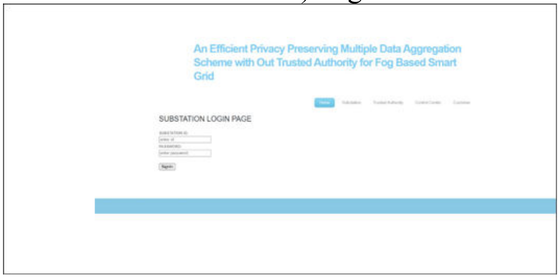
FIGURE: Customer Login Page



An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

Upload Bill

FIGURE: Uploading Bill (File Name Prashanth) Page



An Efficient Privacy Preserving Multiple Data Aggregation Scheme with Out Trusted Authority for Fog Based Smart Grid

SUBSTATION LOGIN PAGE

FIGURE: Substation Login Page

VI. CONCLUSION

In this study, we have proposed a smart and practical PDA scheme with smart pricing and packing method for fog based smart grids, which achieved multifunctional statistics diversified tariffs and efficiency. At first, we have presented a scheme named PDA-SP. With PDA-SP, the CC could provide diversiform pricing strategies, choose a double-winning strategy, and compute more complex and higher-order statistic functions to provide various services. Second, we have presented a scheme named PDA-PM, which could reduce the size of encrypted data and improve performance in performing various secure computations. Moreover, the improved version also could handle general vectors with large entries. At last, the security analysis showed that our proposed scheme was secure against many threats, and the performance evaluation revealed that our proposed scheme was lightweight and efficient.

REFERENCE

[1] Y. Huo, C. Yong, and Y. Lu, “Re-adp: Real-time data aggregation with adaptive-event differential privacy for fog computing,” Wireless Communications and Mobile Computing, vol. 2018, 2018.

[2] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, “A survey on secure data analytics in edge computing,” IEEE Internet of Things Journal, 2019.

[3] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, and K.-C. Li, “A secure fabric blockchain-based data transmission technique for industrial internet-of-things,” IEEE Transactions on Industrial Informatics, 2019.

[4] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, “Querying in internet of things with privacy preserving: Challenges, solutions and opportunities,” IEEE Network, vol. 32, no. 6, pp. 144–151, 2018.

[5] M. Yang, T. Zhu, B. Liu, Y. Xiang, and W. Zhou, “Machine learning differential privacy with multifunctional aggregation in a fog computing architecture,” IEEE Access, vol. 6, pp. 17 119–17 129, 2018.

[6] J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Balancing security and efficiency for smart metering against misbehaving collectors,” IEEE Transactions on Smart Grid, vol. 10, no. 2, pp. 1225–1236, 2017.

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

[8] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, “Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities,”

IEEE Communications Magazine, vol. 56, no. 7, pp. 82–88, 2018.

[9] R. Lu, Privacy-enhancing aggregation techniques for smart grid communications. Springer, 2016.

[10] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, 2011, pp. 113–124.

[11] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, "Prisense: privacy-preserving data aggregation in people-centric urban sensing systems," in 2010 Proceedings IEEE INFOCOM. IEEE, 2010, pp. 1–9.

[12] Q. Li, G. Cao, and T. F. La Porta, "Efficient and privacy-aware data aggregation in mobile sensing," IEEE Transactions on dependable and secure computing, vol. 11, no. 2, pp. 115–129, 2013.

[13] R. Zhang, J. Shi, Y. Zhang, and C. Zhang, "Verifiable privacy-preserving aggregation in people-centric urban sensing systems," IEEE Journal on Selected Areas in Communications, vol. 31, no. 9, pp. 268–278, 2013.

[14] L. Chen, R. Lu, Z. Cao, K. AlHarbi, and X. Lin, "Muda: Multifunctional data aggregation in privacy-preserving smart grid communications," Peer-to- peer networking and applications, vol. 8, no. 5, pp. 777–792, 2015.

[15] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "Ppm-hda: Privacypreserving and multifunctional health data aggregation with fault tolerance," IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940–1955, 2016.

[16] J. Sun, R. Zhang, J. Zhang, and Y. Zhang, "Pristream: Privacy-preserving distributed stream monitoring of thresholded percentile statistics," in IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. IEEE, 2016, pp. 1–9.

[17] H.-Q. Wu, L. Wang, and G. Xue, "Privacy-aware task allocation and data aggregation in fog-assisted spatial crowdsourcing," IEEE Transactions on Network Science and Engineering, 2019.

[18] 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, 2018.

[19] S. Hua, Z. Wu, and S. Jian, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1369–1381, 2017.

[20] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "Effect: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," Science China Information Sciences, vol. 62, no. 3, p. 32103, 2019.

[21] 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.

[22] Y. Chen, J.-F. Mart´ınez-Ortega, P. Castillejo, and L. Lopez, "A ´ homomorphic-based multiple data aggregation scheme for smart grid," IEEE Sensors Journal, vol. 19, no. 10, pp. 3921–3929, 2019.

[23] L. Zhu, M. Li, Z. Zhang, C. Xu, R. Zhang, X. Du, and N. Guizani, "Privacy-preserving authentication and data aggregation for fog-based smart grid," IEEE Communications Magazine, vol. 57, no. 6, pp. 80– 85, 2019.

[24] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999, pp. 223–238.