Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications

[1]Vaishali, [2]Dr Neeta Sharma
[1]M.Tech(SE),School of Engineering & Technology, Noida International University,
Plot 1, Yamuna Expy,Sector 17A, Uttar Pradesh 203201
[2]Assistant Professor, School of Engineering & Technology, Noida International University,
Plot 1, Yamuna Expy, Sector 17A, Uttar Pradesh 203201

Abstract—As the rapid development of 5G and Internet of Things (IoT) techniques, more and more mobile devices with specific sensing capabilities access to the network and large amounts of data. The traditional architecture of the cloud computing cannot satisfy the requirements such as low latency, fast data access for IoT applications. Mobile edge computing can solve these problems, and improve the execution efficiency of the system. In this paper, we propose a privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications. In our model, there are three participants, i.e. terminal device, edge server and public cloud center. The data generated by the terminal devices is encrypted and transmitted to the edge server, then the edge server aggregates the data of the terminal devices and submits the aggregated data to the public cloud center. At last, the aggregated plaintext data can be recovered by public cloud center through its private key. Our scheme not only guarantees data privacy of the terminal devices, but also provides source authentication and integrity. Compared with traditional model, our scheme can save half of communication cost, and is very suitable for mobile edge computing assisted IoT applications.

Index Terms—Cloud computing, Mobile edge computing, Internet of Things (IoT), Data aggregation, Privacy

I. Introduction

Cloud computing [1, 2] has dramatically changed the tradi-tional computing model, which provides users with usable, on-demand access, convenient computing and storage services. By leveraging cloud computing services, enterprises and ordinary users can rent the resources of cloud service provider and do not need to build their own infrastructure. Cloud computing is widely accepted due to the features of flexibility, easy to use, high scalability, location independence and reliability. Meanwhile, with the development of sensing technology and microelectronics technology, the Internet of Things (IoT) [3, 4] allows any device to access the Internet. In the IoT vision, the object can be identified by radio-frequency identification (RFID) technique [5], and the environment parameters can be sensed by wireless sensor networks (WSN) [6]. Then, the various smart applications, such as smart grid, smart home, smart city, and intelligent agriculture, can be built by analyzing and utilizing the sensory data. Take intelligent agriculture as an example, the crop growth environment information can be obtained by different types of sensors (environmen-tal temperature and humidity, soil moisture, carbon dioxide, images, etc.) deployed at the agricultural production sites. Then the sensory data collected and analyzed by the control center, and the corresponding operations such as irrigation, cooling, fertilization and spraying can be done according to the feedback of all kinds of collected information. To take complementary advantages of the IoT and cloud, researcher have proposed the concept of cloud assisted IoT [7–10]. In the new paradigm, IoT is no longer restricted by the storage, communication and processing capacities, which are compensated by the could. On the contrary, the cloud can deal with more real life applications in a more distributed and dynamic way by combine with the IoT. Different organizations have predicted that billions of smart devices will be connected to the Internet in near future [11], and will generate huge amount of data, which should be analyzed and processed in a security and effective way. Besides, the widespread applications of IoT require the smart devices to have low latency, high data rate, fast data access for real-time data processing/analysis and decision making [12]. However, the traditional cloud computing cannot satisfy these requirements, and the concept of mobile edge computing (MEC) [13–15] was proposed by researchers. A typical architecture of mobile edge computing assisted IoT applications is shown in Figure 1. It is a three-level hierarchy that contains the Cloud, MEC and terminal devices. The terminal devices can be the mobile devices, sensors and wearable devices with communication and sensing capabilities. Compared to IoT terminal devices, more computing, storage and communication resources are available on the edge server. The edge server can be a stand-alone server or a gateway device, which is deployed at the edge of a cloud computing network and physical proximity to the IoT terminal devices, and plays as the bridge between

This work was supported supported by the Hunan Provincial Natural Science Foundation of China under Grant 2018JJ3191, the Open Foundation of State key Laboratory of Networking and Switching Technology, Beijing U-niversity of Posts and Telecommunications, under Grant SKLNST-2018-1-12, the National Natural Science Foundation of China under Grant 61772194 and Grant 61572013, the National Funding from the FCT-Fundac¸ao˜ para a Cienciaˆ e a Tecnologia through the UID/EEA/50008/2013 Project, by Finatel through the Inatel Smart Campus project; by Finep, with resources from Funttel, Grant No. 01.14.0231.00, under the Centro de Referncia em Radiocomunicac¸oes˜-CRR project of the Instituto Nacional de Telecomunicac¸oes˜ (Inatel), Brazil. (Corresponding author: Xiong Li.)

X. Li is with the School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China, and also with State key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China (e-mail: lixiongzhq@163.com).

S. Liu is with the School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China (e-mail: liushanpeng123@outlook.com).

F. Wu is with the Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China (e-mail: conjur-er1981@gmail.com).

S. Kumari is with the Department of Mathematics, Ch. Charan Singh University, Meerut, 250005, India (e-mail: saryusiirohi@gmail.com).

J. J.P.C. Rodrigues is with the National Institute of Telecommunica-tions (Inatel), Santa Rita do Sapuca´ı, MG, Brazil; and with Instituto de Telecomunicac¸oes,˜ Portugal; University of Fortaleza (UNIFOR), Fortaleza, CE, Brazil (e-mail: joeljr@ieee.org).

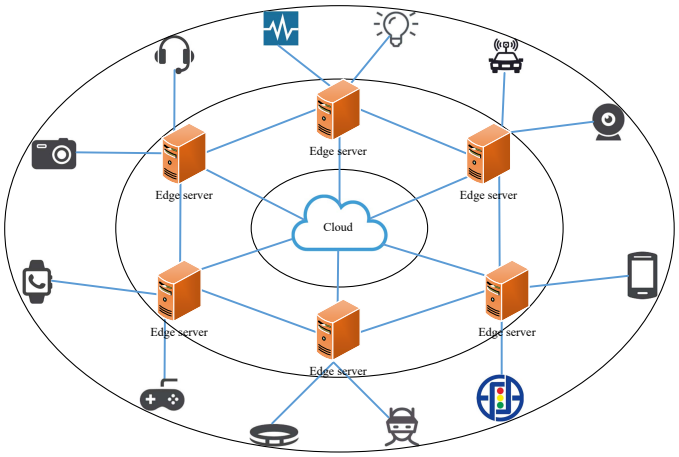

Fig. 1: Typical architecture of MEC assisted IoT applications

IoT terminal devices and public cloud center. Edge computing allows some computations and processing to be performed at the edge of the network, thus improving the efficiency of the traditional cloud computing. The edge server not only performs computing offloading, data storage and processing, but also delivers services from the cloud to the user. Some previous work [16–18] had proved that the edge computing greatly reduces the response time and the energy consumption compared to the traditional could computing. Therefore, the mobile edge computing has a wide range of applications, such as healthcare [19], video analytics, mobile big data analytics, connected vehicles, smart grid, smart building control, ocean monitoring. Take MEC based healthcare application as an example, MEC device can collect vital signs parameters of the patient from medical sensor or wearable devices and submit it to the medical cloud center for storage and sharing. Medical professionals can access these data and make timely diagnosis for patients. However, due to the complexity and real-time feature of the MEC service model, the multi-source heterogeneity and the resource-constrained of the terminal devices, the data security and privacy protection mechanisms in the traditional cloud computing environment are no longer applicable to MEC. The security of data storage, sharing, computing, and privacy protection are becoming more and more prominent. [20, 21] have pointed out the security and privacy issues of mobile edge computing.

In this paper, we consider the scenario of mobile edge computing assisted Internet of Things. Via the edge computing, the public cloud center can utilize the sensing function of the IoT terminal devices to acquire the special parameters. The data collected by the terminal devices is aggregated by the edge servers, and finally the public cloud center can get the total aggregated palaintext from the aggregated ciphertext data from edge servers. Such as counting the frequency of occurrence of specific abnormal situation in a very large area. In this case, it requires that the total result can only be obtained by the public cloud center, and privacy of the terminal devices should be ensured. To achieve this purpose, we first introduce the privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications. Then we give the system model and security model, and design a privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications based on the Boneh-Goh-Nissim cryptosystem [22].

The remaining chapters are arranged as follows. Section II and section III introduce the related work and the cryptography basis of our scheme, respectively. The system model, security model and the definition of our scheme are given in section IV. The proposed privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications is described in section V. Section VI and VII evaluate the security features and performance of the proposed scheme, respectively. Finally, section VIII concludes the full paper.

II. Related work

As an is important research content of information systems, data aggregation can provide comprehensive and accurate data for information systems, and enhances the reliability and accuracy of the system. In the IoT environments, the data collected by adjacent sensors is typically redundant and highly correlated. Data aggregation is an effective mechanism to combine these redundant data into high-quality information, and saves energy and bandwidth consumption, thus extends the lifecycle of the system. Besides, the privacy preserving data aggregation become a research concern due to it can guarantee the privacy of sensitive data during the data aggregation processes. Researchers have studied the data aggregation schemes for WSN [23–25], mobile sensing system [26–28] and smart grid [29–31]. For WSN, researchers have proposed many aggregation schemes based on network topologies, such as tree, cluster and ring topologies. In 2014, Roy et al. [23] proposed and synopsis diffusion based secure data aggregation for ring topology WSN, it addresses the communication loss problem. Later, Shin and Park [24] presented an homomorphic encryption based data aggregation scheme for heterogeneous clustered WSN, it can resist some attacks, but cannot ensure the integrity of the data. Recently, by employing identity-based cryptography, Shen et al. [25] proposed a secure data aggregation for WSN, which mainly solved coalition attack. Compared to the WSN, due to the network topology is not fixed and the participants costs should be compensated, the design of data aggregation for mobile sensing system is a more challenging thing. In 2013, Zhang et al. [26] proposed a verifiable privacy-preserving aggregation scheme (PPAS) for urban sensing systems. However, it needs a trusted hardware and an additional communication to protect data integrity. Later, Li et al. [27] proposed an efficient PPAS in mobile sensing, which adopted the idea of multi-secret sharing. However, the existence of the trusted key dealer and the adjust problem of the shares if a user leaves make it lacks efficiency and flexibility. In 2016, Jin et al. [28] proposed a privacy-preserving data aggregation framework for mobile sensing system that integrates incentives, data aggregation, and data perturbation mechanisms. In 2012, Lu et al. proposed an PPAS for smart grid communication by using Paillier's homomorphic encryption [32]. Later, Fan et al. proposed an PPAS for smart grid to against internal attackers. Recently, Wang [31] proposed an identity-based

data aggregation protocol for smart grid to against malicious tampering attack. In the mobile edge computing environment, data aggregation can save communication overhead between edge server and public cloud center, and saves the computing resources of public cloud center. It is especially suitable for the tasks assigned by the public cloud center to the terminal devices via the edge server, where the partial results should be added to the total results [33]. To ensure the security of data aggregation, the terminal device's data should be encrypted before submission, and the edge server should be able to aggregate the data on ciphertext form. Obviously, the traditional encryption algorithm cannot achieve this function, while homomorphic encryption [32, 34] allows us to perform special algebraic operations on ciphertext, and its result is the same as performing the same operation on the plaintext and then encrypting it. In current society, privacy is getting more and more people's attention. In mobile edge computing, user privacy is still a challenge, i.e. the terminal users should share their sensed data for the services, while these data may deduce the leakage of the privacy [35]. Therefore, the data aggregation scheme should ensure the privacy of the terminal devices, i.e. the public cloud center cannot retrieve special data of terminal devices from the aggregation data.

III. Preliminaries

In this section, we briefly introduce two preliminaries, i.e. the bilinear map of composite order groups [22] and the Boneh-Goh-Nissim cryptosystem [22], which are used as the basis of the proposed scheme.

A. Bilinear map of composite order groups

For a input of security parameter $\tau \in Z^+$, an algorithm $\mathcal{G}$ outputs a tuple (p, q, G, G_1, e), where p, q are two random large prime numbers with τ-bit length, G, G_1 are two cyclic groups of order $N = pq$, and $e : G \times G \to G_1$ is bilinear map with the following properties:

1) Bilinearity: $\forall u, v \in G$, and $a, b \in Z_N$, $e(u^a, v^b) = e(u, v)^{ab}$;
2) Non-degeneracy: if g is a generator of G, $e(g, g)$ is a generator of G_1, and $e(g, g) \neq 1_{G_1}$;
3) Computability: $\forall u, v \in G$, there is an efficient algorithm to compute $e(u, v)$.

B. Boneh-Goh-Nissim cryptosystem

Boneh-Goh-Nissim cryptosystem [22] is widely used in privacy preserving applications due to its homomorphic properties. It contains three algorithms, i.e. key generation, encryption and decryption, and we illustrate this cryptosystem as below:

1) Key generation: For a security parameter $\tau \in Z^+$, the system parameters (p, q, G, G_1, e) described above are generated by $\mathcal{G}$. Two random generators g, x of G are chosen, and $h = x^q$ is calculated. Note that h is a generator of the subgroup of G with order p. The public key of the system is $PK = \{N, G, G_1, e, g, h\}$, where $N = pq$, and private key $SK = p$ is kept secretly.
2) Encryption: For a message $m \in [0, T], T < q$, a random number $r \in [0, N - 1]$ is chosen, and the ciphertext is calculated as $C = g^m h^r$.
3) Decryption: To decrypt the ciphertext C using the secret key $SK = p$, compute $C^p = (g^m h^r)^p = g^{mp} x^{pq} = (g^p)^m$. Let $\hat{g} = g^p$, then $C^p = \hat{g}^m$, and m can be recovered by sloving the discrete logarithm using Pollard's lambda method [36].

IV. System and security models of the proposed scheme

In this section, we introduce the system model, phases and security model of the proposed scheme.

A. System model

There are three entities involved in the proposed scheme, i.e. the Terminal Device (TD), Edge Server (ES) and Public Cloud Center (PCC):

1) TD: TDs are user's devices, such as the mobile phone and the IoT devices, which are connected to the edge network to collect specific data. These devices usually have limited computing and communications resources.
2) ES: ESs are maintained by PCC, and located at the proximity of TDs (edge of the network). ESs bridge the TDs and PCC to extend the applications of cloud services by providing store and processing services for the TDs.
3) PCC: PCC provides cloud computing and storage services for the users with large storage capacity and strong computing power. The data from TDs and ESs can be stored and processed on PCC. PCC initializes the system by generating system parameters. Besides, PCC is responsible for the registration of TDs and generates the private/public keys for ESs.

The communication model of our system is shown in Figure 2. First, TD encrypts the collected data and generates the corresponding signature using the secret key. Then TD transmits the ciphertext and the signature to the edge server. When receiving the data of all terminal devices, ES verifies the validity of these messages using the terminal devices' public keys. Then, ES aggregates these ciphertext and produces the corresponding signature, and submits the aggregated data with the signature to PCC. After the edge servers' aggregated data is verified, PCC can retrieve the aggregated plaintext using own secret key. In general applications of mobile edge computing, the communications between PCC and ESs, and ES and the corresponding TDs are both two-way. Such as in mobile edge computing based data storage, TD can upload the data to PCC via ES, and also can download the data from PCC via ES.

B. Definition of the proposed scheme

Our scheme contains five phases as below:

1) Initialization: On input the security parameters, PCC generates the system parameters. PCC also generates private/public key pairs for itself and ESs, and then

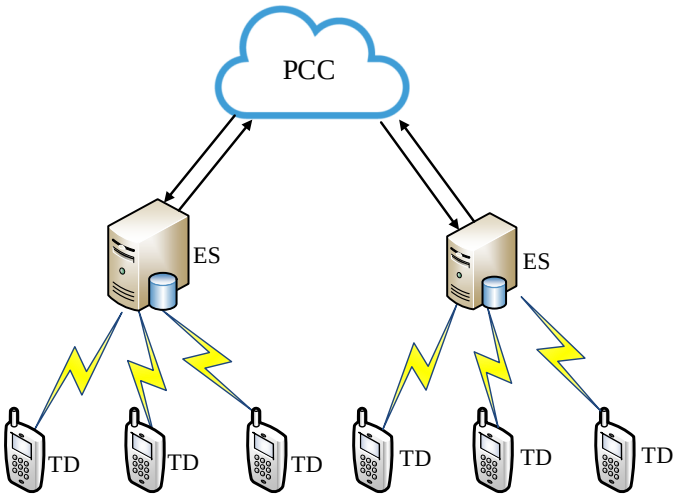

Fig. 2: Communication model of our scheme

deploys the ESs in the edge of the network. Finally, PCC publishes the public parameters of the system.

2) Registration: TD chooses the identity, generates the private/public key pair, and registers to the PCC by using the signature of its identity and private key. PCC accepts the registration if the signature is verified by the public key.
3) TD data encryption and report: For the data to be uploaded, TD encrypts it and generates the corresponding signature. Then TD reports the ciphertexts and the signature to its ES.
4) ES data aggregation and report: First, each ES checks the validity of the ciphertexts reported by TDs, and aggregates the ciphertexts received from TDs to a ciphertext if they are valid. Then, each ES generates a signature for the aggregated ciphertext, and reports the aggregated ciphertext with the signature to PCC.
5) Decryption: PCC checks the validity of the ciphertexts reported by ESs, and performs the decryption process using secret key and recover the aggregated plaintext.

C. Security requirements

A privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications should not only satisfy some security requirements, but also maintain efficiency. We illustrate the security requirements of the scheme as below:

1) Privacy: The transmitted data contains important privacy information of the user, such as it may relate to user's consumer habits and personal preferences. So a preserving data aggregation scheme for mobile edge computing assisted IoT applications should protect the privacy of the data, and neither the internal adversaries nor the external adversaries cannot recover the user's data from the cipertexts transmitted via public channel.
2) Integrity: The integrity of the data reported by TD to ES, and the aggregation data reported by ES to PCC can be ensured, i.e. any modification of the data can be detected by ES or PCC.
3) Source authentication: A preserving data aggregation scheme for mobile edge computing assisted IoT applications should provide the source authentication, i.e. the ES can check if the data generated by a legal TD, and the PCC can check if the received aggregation data submitted from a legal ES.

V. The Proposed Scheme

In this section, we design a privacy preserving data aggregation scheme for mobile edge computing by using the bilinear map of composite order groups and Boneh-Goh-Nissim cryptosystem. The five phases of our scheme as defined in section IV-B are illustrated as below, and the notations and their description of the paper are listed in Table I.

TABLE I: Notations

Notation	Description
PCC	The public cloud center
ES_i	The i-th edge server
TD_{ij}	The j-th terminal device accesses to ES_i
ID_{ES_i}	The identity of ES_i
$ID_{TD_{ij}}$	The identity of TD_{ij}
p, q	Two τ bits large prime numbers
G, G_1	Two cyclic groups of order $N = pq$
e	Bilinear pairing $e : G \times G \to G_1$
f, g, x	Three generators of G
$\hat{g}$	$\hat{g} = g^p$
$h = x^q$	A generator of the subgroup of G with order p
H	A secure hash function $H : \{0,1\}^* \to G$
(y_i, Y_i)	The private/public key pair of ES_i, $Y_i = h^{y_i}$
(y_{ij}, Y_{ij})	The private/public key pair of TD_{ij}, $Y_{ij} = h^{y_{ij}}$
r_i, r_{ij}	The random numbers chosen by ES_i and TD_{ij}
t_i, t_{ij}	Timestamps of ES_i and TD_{ij}
C_i, C_{ij}	Ciphertexts generated by ES_i and TD_{ij}
σ_i, σ_{ij}	Signatures generated by ES_i and TD_{ij}

A. Initialization

To initialize the system, PCC needs select some parameters. On input the security parameter τ, PCC generates the parameters (p, q, G, G_1, e) as shown in section III-A by using algorithm $\mathcal{G}$. Next, PCC chooses three random generators f, g and x of G, and calculates $N = pq$ and $h = x^q$. Then, PCC chooses a secure hash function $H : \{0,1\}^* \to G$. Finally, PCC publishes the public key $(N, G, G_1, e, f, g, h, H)$ of the system, and keeps the private key p secretly.

B. Registration

The PCC chooses an identity ID_{ES_i}, and generates the private/public key pair (y_i, Y_i) for ES_i $(i = \{1, 2, \cdots n\})$, where $y_i \in (1, p)$ and $Y_i = h^{y_i}$. Then, PCC stores the pairs (ID_{ES_i}, Y_i) in its database, and stores (ID_{ES_i}, y_i, Y_i) in the ES_i. Finally, the edge servers ESs are deployed at the edge of the network, and they keep their private keys secretly.

When a user with a $TD_{ij} (j = 1, 2, \cdots, l)$ wants to access the location proximity edge server ES_i, the registration phase should be performed. The user chooses an identity $ID_{TD_{ij}}$, and generates the private/public key pair (y_{ij}, Y_{ij}), where y_{ij} is a random number with bit length of $1 \sim \tau - 1$, and $Y_{ij} = h^{y_{ij}}$. Then $ID_{TD_{ij}}$ gets current timestamp t_{Reg} and calculates $Sig_{ij} = H(ID_{TD_{ij}} \| t_{Reg})^{y_{ij}}$, and submits

$\{ID_{TD_{ij}}, t_{Reg}, Sig_{ij}, Y_{ij}\}$ to PCC for registration. When receiving the registration request, PCC first checks the freshness of the timestamp t_{Reg}, and then checks $e(Sig_{ij}, h) \stackrel{?}{=} e(H(ID_{TD_{ij}} \| t_{Reg}), Y_{ij})$. If it does not hold, PCC rejects the request. Otherwise, $ID_{TD_{ij}}$ is registered successfully. PCC stores $\{ID_{TD_{ij}}, Y_{ij}\}$ in its database and the corresponding ES_i.

Besides, for a edge server ES_i and its l terminal servers $TD_{ij} (j = 1, 2, \cdots, l)$, PCC generates l random numbers $\{\pi_{i1}, \pi_{i2}, \cdots, \pi_{il}\}$ from Z_N, and calculates $\pi_i = -(\pi_{i1} + \pi_{i2} + \cdots + \pi_{il}) \bmod N$. Then, PCC assigns π_i to ES_i and π_{ij} to the corresponding TD_{ij} $(j = 1, 2, \cdots, l)$ secretly, and deletes these information.

C. TD data encryption and report

In this phase, each $TD_{ij} (j = 1, 2, \cdots, l)$ encrypts the message m_{ij} and generates the corresponding signature, and the reports these information to its edge server $ES_i (i = \{1, 2, \cdots n\})$.

When collects the usage data $m_{ij} \in [0, T]$, TD_{ij} chooses a random number r_{ij}, and calculates the ciphertext $C_{ij} = f^{\pi_{ij}} g^{m_{ij}} h^{r_{ij}}$. Then, TD_{ij} acquires the current timestamp t_{ij}, and generates a signature for the ciphertext $\sigma_{ij} = H(ID_{TD_{ij}} \| C_{ij} \| t_{ij})^{y_{ij}}$ using its secret key y_{ij}. Finally, TD_{ij} reports the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ to its edge server ES_i.

D. ES data aggregation and report

In this phase, each ES verifies the messages collected from its TDs, and then aggregates these messages and reports the aggregation data to PCC. Here, we take ES_i as an example to illustrate this phase.

When receiving all the messages reported by TD_{ij} $(j = 1, 2, \cdots, l)$, ES_i checks the validity of $ID_{TD_{ij}}$ and verifies the freshness of the timestamp t_{ij} $(j = 1, 2, \cdots, l)$. The messages will be discarded if one is failure. Then ES_i performs the batch verification $e(\prod_{j=1}^{l} \sigma_{ij}, h) \stackrel{?}{=} \prod_{j=1}^{l} e(H(ID_{TD_{ij}} \| C_{ij} \| t_{ij}), Y_{ij})$, which greatly reduces the ES_i's computing and communication costs. If it does not hold, at least one of the message reported by TD_{ij} $(j = 1, 2, \cdots, l)$ is invalid, and ES_i can find the invalid messages by checking $e(\sigma_{ij}, h) \stackrel{?}{=} e(H(ID_{TD_{ij}} \| C_{ij} \| t_{ij}), Y_{ij})$ $(j = 1, 2, \cdots, l)$. On the contrary, the messages reported by TD_{ij} $(j = 1, 2, \cdots, l)$ are all valid. Then, ES_i aggregates the received messages as $C_i = f^{\pi_i} \prod_{j=1}^{l} C_{ij}$. Then ES_i acquires the current timestamp t_i, and generates a signature for the aggregated data $\sigma_i = H(ID_{ES_i} \| C_i \| t_i)^{y_i}$. Finally, ES_i submits the message $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ to the PCC.

Please note that

$$\begin{aligned} C_i &= f^{\pi_i} \prod_{j=1}^{l} C_{ij} \\ &= f^{\pi_i} f^{\sum_{j=1}^{l} \pi_{ij}} g^{\sum_{j=1}^{l} m_{ij}} h^{\sum_{j=1}^{l} r_{ij}} \\ &= f^{\pi_i + \sum_{j=1}^{l} \pi_{ij}} g^{\sum_{j=1}^{l} m_{ij}} h^{\sum_{j=1}^{l} r_{ij}} \\ &= f^{0} g^{\sum_{j=1}^{l} m_{ij}} h^{\sum_{j=1}^{l} r_{ij}} \\ &= g^{\sum_{j=1}^{l} m_{ij}} h^{\sum_{j=1}^{l} r_{ij}} \end{aligned}$$

E. Decryption

When receiving the messages reported by n edge servers $\{ES_1, ES_2, \cdots, ES_n\}$, PCC checks the validity of ID_{ES_i} and verifies the freshness of the corresponding timestamp t_i $(i = 1, 2, \cdots, n)$. The messages will be discarded if one is failure. Then PCC performs batch verification $e(\prod_{i=1}^{n} \sigma_i, h) \stackrel{?}{=} \prod_{i=1}^{n} e(H(ID_{ES_i} \| C_i \| t_i), Y_i)$, which greatly reduces the PCC's computing and communication costs. If it does not hold, at least one of the message reported by ES_i $(i = 1, 2, \cdots, n)$ is invalid, and PCC can find the invalid messages by checking $e(\sigma_i, h) \stackrel{?}{=} e(H(ID_{ES_i} \| C_i \| t_i), Y_i)$ $(i = 1, 2, \cdots, n)$. On the contrary, the messages reported by ES_i $(i = 1, 2, \cdots, n)$ are all valid. Then, PCC aggregates the received messages as

$$C = \prod_{i=1}^{n} C_i = g^{\sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}} h^{\sum_{i=1}^{n} \sum_{j=1}^{l} r_{ij}}.$$

Since $h^p = (x^q)^p = x^{pq} = 1$, by taking the secret key p, PCC can calculate

$$\begin{aligned} V &= C^p = (\prod_{i=1}^{n} C_i)^p \\ &= (g^{\sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}} h^{\sum_{i=1}^{n} \sum_{j=1}^{l} r_{ij}})^p \\ &= g^{p \sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}} \\ &= \hat{g}^{\sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}} \end{aligned}$$

Then, PCC can recover the aggregated plaintexts of the TDs $\sum_{i=1}^{n} \sum_{j=1}^{l} m_{ij}$ by solving discrete logarithm using Pollard lambda method.

We also show the last three phases of our scheme in Figure 3.

VI. Security analysis

In this section, we analyze the security features of the proposed scheme and show that it meets the security requirements defined above.

A. Privacy Protection

The main purpose of privacy protection is to avoid the leakage of TD_i's usage data, and we consider this feature from two aspects, i.e. the external attack and internal attack.

TD_{ij}	For $m_{ij} \in [0, T]$, generates a nonce r_{ij}
TD data encryption	Calculates $C_{ij}=f^{\pi_{ij}} g^{m_{ij}} h^{r_{ij}}$
and report phase	Gets the timestamp t_{ij}
	Generates a signature $\sigma_{ij}=H(ID_{TD_{ij}} \| C_{ij} \| t_{ij})^{y_{ij}}$
	Submits $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ to ES_i
ES_i	Checks the validity of $ID_{TD_{ij}}$
ES data aggregation	Performs batch verification $e(\prod_{j=1}^{l} \sigma_{ij}, h) ?= \prod_{j=1}^{l} e(H(ID_{TD_{ij}} \| C_{ij} \| t_{ij}), Y_{ij})$
and report phase	Aggregates the messages $C_i=f^{\pi_j} \prod_{j=1}^{l} C_{ij}$
	Gets the timestamp t_i
	Generates a signature $\sigma_i=H(ID_{ES_i} \| C_i \| t_i)^{y_j}$
	Submits $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ to *PCC*
PCC	Checks the validity of ID_{ES_i}
Decryption phase	Performs batch verification $e(\prod_{i=1}^{n} \sigma_i, h) ?= \prod_{i=1}^{n} e(H(ID_{ES_i} \| C_i \| t_i), Y_i)$
	Aggregates the messages $C=\prod_{i=1}^{n} C_i = g^{\sum_{i=1}^{n}\sum_{j=1}^{l} m_{ij}} h^{\sum_{i=1}^{n}\sum_{j=1}^{l} r_{ij}}$
	Calculates $V=C^p=(\prod_{i=1}^{n} C_i)^p=(g^{\sum_{i=1}^{n}\sum_{j=1}^{l} m_{ij}} h^{\sum_{i=1}^{n}\sum_{j=1}^{l} r_{ij}})^p$ $=g^{p\sum_{i=1}^{n}\sum_{j=1}^{l} m_{ij}}=\hat{g}^{\sum_{i=1}^{n}\sum_{j=1}^{l} m_{ij}}$
	Recovers the aggregated plaintexts $\sum_{i=1}^{n}\sum_{j=1}^{l} m_{ij}$ by solving discrete logarithm using Pollard Lambda method

Fig. 3: The proposed scheme

First, an external attacker can eavesdrop the messages transmitted from TD_{ij} to ES_i, and from ES_i to PCC. Suppose that the external attacker has eavesdropped the TD_{ij}'s message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$, where the ciphertext is $C_{ij} = f^{\pi_{ij}} g^{m_{ij}} h^{r_{ij}}$. However, due to the Boneh-Goh-Nissim cryptosystem is semantic secure against the chosen ciphertext attack, the external attacker cannot retrieve TD_{ij}'s usage data m_{ij} without known π_{ij} and r_{ij}. Besides, if ES_i's aggregated data $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ has been eavesdropped by an external attacker, where $C_i = g^{\sum_{j=1}^{l} m_{ij}} h^{\sum_{j=1}^{l} r_{ij}}$, the attacker cannot even get the sum of l user's usage data $\sum_{j=1}^{l} m_{ij}$ without known PCC's secret key p, not to mention the single user usage data m_{ij}. Therefore, the proposed scheme can preserve user's privacy to against external attack.

Second, an internal attacker who accesses the secret keys of ESs or PCC may want to recover the usage data of TDs. Suppose that the internal attacker has eavesdropped the TD_{ij}'s message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$, where the ciphertext is $C_{ij} = f^{\pi_{ij}} g^{m_{ij}} h^{r_{ij}}$. Even though the attacker acquired PCC's secret key p, then can calculate $C_{ij}^p = f^{\pi_{ij} p} g^{m_{ij} p} h^{r_{ij} p} = f^{\pi_{ij} p} \hat{g}^{m_{ij}}$. However the security of m_{ij} is ensured by the secret information π_{ij}, which can be considered as a blinding factor to avoid the leakage of the usage data. Therefore, the proposed scheme also can preserve user's privacy to against internal attack.

B. Integrity

Data integrity is an important property of information security, which ensures the data is not destroyed or tampered during the transmission. The proposed scheme can guarantee the data integrity of the transmitted messages, and the tampered messages can be detected by ES or PCC.

For the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ received by ES_i which was reported by TD_{ij}, ES_i first checks the validity of the identity and the freshness of timestamp, and then the integrity of the message can be verified by checking if $e(\sigma_{ij}, h) = e(H(ID_{TD_{ij}} \| C_{ij} \| t_{ij}), Y_{ij})$ is hold. As we can see that each element of the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ is involved in the integrity verification, any tampering with the message will cause the equation not to hold. Therefore, the integrity of the message reported by TD_{ij} can be checked by ES_i. Similarly, when receiving the message $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ reported by ES_i, the integrity of the message can be verified by PCC by checking if the equation $e(\sigma_i, h) = e(H(ID_{ES_i} \| C_i \| t_i), Y_i)$ $(i = 1, 2, \cdots, n)$ is hold. Any tampering with the message will cause the equation not to hold since each part of $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ is involved in the integrity verification. Therefore, the PCC can check the data integrity of the messages reported by ESs.

C. Source authentication

As discussed in the above subsection, the validity of the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ reported by TD_{ij} can be verified by ES_i, and $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ reported by ES_i can be verified by PCC. As we can see that identities $ID_{TD_{ij}}$ and ID_{ES_i} are contained in the messages $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ and $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$, respectively. Therefore, the ES_i and PCC can make sure the source of the messages. Specifically, the ES_i and PCC can confirm the invalid messages sent by which TD_{ij} and ES_i, respectively. Besides, TD_{ij} and ES_i's signatures $\sigma_{ij} = H(ID_{TD_{ij}} \| C_{ij} \| t_{ij})^{y_{ij}}$ and $\sigma_i = H(ID_{ES_i} \| C_i \| t_i)^{y_i}$ are generated based on the corresponding secret keys y_{ij} and y_i, respectively. Therefore, any adversary without y_{ij} and y_i cannot forge the correct messages $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ and $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ to imitate TD_{ij} and ES_i, respectively. Therefore, the proposed scheme provides the proper source authentication for all transmitted messages.

VII. Performance evaluation

In this section, we evaluate the performance of the proposed scheme with two recent schemes about data aggregation [31, 33], and mainly consider two aspects, i.e. the computation cost and communication cost. We test the time cost of referring cryptographic operations on the platform same as in [37]. Some data are from there, and we give the concrete time in Table II. Some illustrations are listed as follows. T_{e2} is the double exponetiation in the cyclic group, e.g., $g^a h^b$. To evaluate the communication cost of the proposed scheme, we assume that the large prime numbers p and q are both 512 bits, and therefore, the bit length of N is 1024. So the length of elements in G and G_1 are 1024 bits, and the elements on point on elliptic curve is 320 bits, same as the current RSA security level. Moreover, the lengths of timestamp and identity are 64 and 32 bits, respectively.

A. Computation cost

To evaluate the computation cost of the proposed scheme with other related schemes [31, 33], we assume that there are n ES and each ES contains l TD in the data aggregation schemes.

In the proposed scheme, TD_{ij} needs $2T_{e2}$ to generate the ciphertext C_{ij} and $T_{mp} + T_e$ to generate the corresponding

TABLE II: Time cost of referring cryptographics

Symbol	Meaning	Time (ms)
T_p	time of bilinear pairing	13.6736
T_{e2}	time of double exponentiation	0.4139
T_e	time of exponentiation	0.3418
T_s	time of scalar multiplication	0.2986
T_{mp}	time of map to point	0.6272
T_i	time of inversion in cyclic group	0.0256
T_m	time of multiplication in group	0.0019

signature σ_{ij}. Therefore, the total computation cost of each TD is $2T_{e2} + T_{mp} + T_e = 1.7968$ ms. Each ES needs $(l+1)T_p + 2(l-1)T_m + lT_{mp}$ to perform batch verification, $T_e + lT_m$ to generate the aggregated data, and $T_{mp} + T_e$ for the corresponding signature σ_i. Therefore, the total computation cost of each ES is $(T_p + 3T_m + T_{mp})l + T_p - 2T_m + 2T_e = (14.3065l + 14.3534)$ ms. Besides, the PCC needs $(n+1)T_p + 2(n-1)T_m + nT_{mp}$ to perform the batch verification, $(n-1)T_m$ to aggregate the messages, and T_e to calculate V, so the total computation cost of PCC is $(T_p + 3T_m + T_{mp})n + T_p - 3T_m + T_e) = 14.3065n + 14.0097$ ms.

In Wang et al.'s scheme [33], TD needs $T_e + T_{e2}$ to generate the ciphertext c_i, $T_{mp} + T_s$ to generate the signature σ_i, and $2T_p + T_{mp}$ to verify the equation. Therefore, the total cost of TD is $T_e + T_{e2} + 2T_{mp} + T_s + 2T_p = 29.6559$ ms. Each ES needs $(2T_p + T_{mp})l$ to verify all queries, $2T_p + lT_{mp}$ to verify the validity of l messages, $2(l-1)T_m$ to aggregate the messages, and $T_{mp} + T_s$ to create the signature. So the total cost of ES is $(2T_p + 2T_{mp} + 2T_m)l + 2T_p - 2T_m + T_{mp} + T_s = 28.6054l + 28.2692$ ms. The PCC needs $(2T_p + T_{mp} + T_e + T_i + T_m)n = 28.3437n$ ms to verify the messages and recover the plaintext.

In Wang's scheme [31], TD needs $2T_e + T_{e2} + T_{mp} + T_m = 1.7266$ ms to generate the ciphertext and the corresponding signature. ES needs $(3T_e + 3T_m + 2T_{mp} + T_p)l - 2T_m + 2T_p$ to perform the batch verification and $(2l-1)T_m + 2T_e + T_{mp}$ to generate the aggregated ciphertext and the corresponding signature. Therefore, the total computation cost of ES is $(3T_e + 5T_m + 2T_{mp} + T_p)l - 3T_m + 2T_p + 2T_e + T_{mp} = 15.9629l + 28.6523$ ms. The PCC needs $(4T_p + 2T_{mp} + 2T_m + T_i)n = 55.9782n$ ms to verify the signatures and recover the plaintext.

From the above analysis, we see that the time cost of our scheme on TD is in the middle, but is only a little more than [31]. Besides the time cost comparison results on ES side and PCC side can be seen in Figure 4 and Figure 5, respectively. From theses two figures, we can see that the time cost on ES and PCC in our scheme is the least among the three schemes. As a data aggregation scheme, it is important to save time on the aggregation part. So our scheme performs better than the other two.

B. Communication cost

To evaluate the communication cost of the proposed scheme with other related schemes [31, 33], we also assume that there are n ES and each ES contains l TD in the data aggregation schemes. The communication of the proposed scheme contains two parts, i.e. TD reports the message to

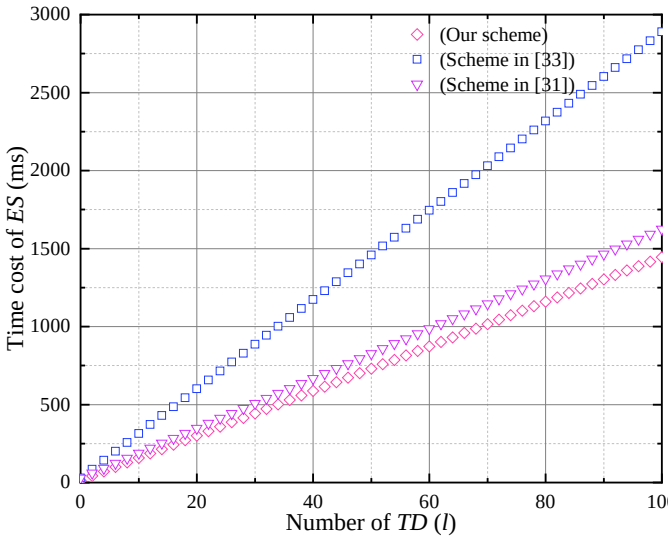

Fig. 4: Time cost comparison on ES side

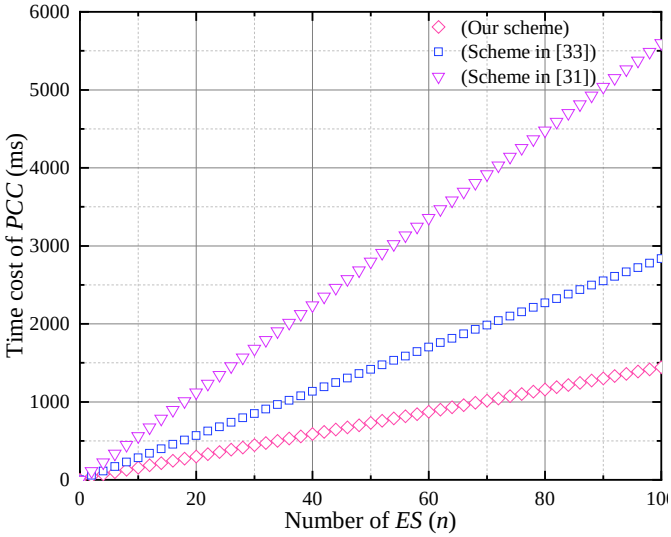

Fig. 5: Time cost comparison on PCC side

ES, and ES reports the aggregated data to PCC. In the TD data encryption and report phase, TD_{ij} reports the message $\{ID_{TD_{ij}}, t_{ij}, C_{ij}, \sigma_{ij}\}$ to ES_i, and the communication overhead is $64 + 32 + 1024 + 1024 = 2144$ bits. Besides, in ES data aggregation and report phase, ES_i reports the aggregated message $\{ID_{ES_i}, C_i, \sigma_i, t_i\}$ to PCC, and the communication overhead is $64 + 1024 + 1024 + 32 = 2144$ bits. Therefore, in one session of data aggregation, the communications cost of TD_{ij} and ES_i are both 2144 bits, so the total communication cost of one session is $2144nl + 2144n$ bits.

In Wang et al.'s scheme [33], we assume that the bit length of the authorization information Au is 32. In their scheme, TD should send $32 + 32 + 1024 = 1088$ bits query data to ES and ES should response $32 + 32 + 1024 = 1088$ bits data to complete the authentication. Furthermore, TD should submit $2048 + 32 + 64 + 1024 = 3168$ bits data to ES for one ciphertext. Therefore the total communication cost between TD and ES of TD data processing and upload

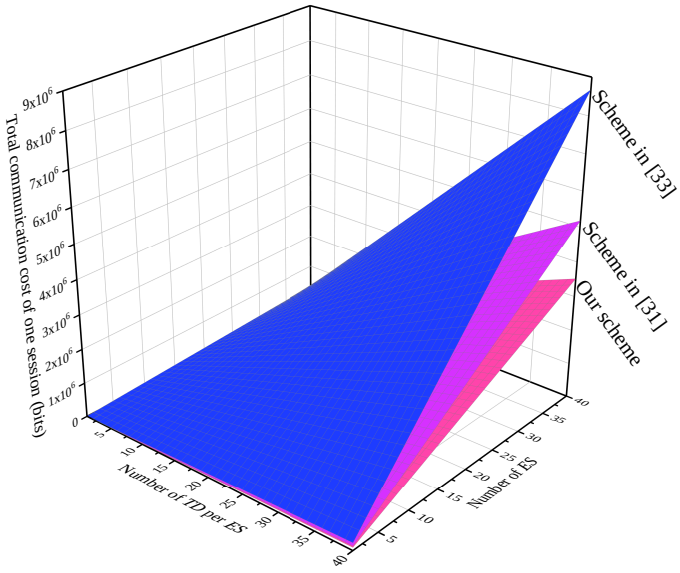

Fig. 6: Communication cost comparison

phase is $1088 + 1088 + 3168 = 5344$ bits. Besides, in secure data aggregation and upload, each ES should submit $2048 + 32 + 32 + 64 + 1024 = 3200$ bits data to PCC. Therefore, the total communication cost of one session is $5344nl + 3200n$ bits.

In the scheme of [31], each TD should submit $2048 + 1024+64 = 3136$ bits data to ES, and each ES should submit $2048 + 2048 + 64 = 4160$ bits data to PCC. Therefore, the total communication cost of one session is $3136nl + 4160n$ bits.

From the above analysis, there is no doubt that our scheme costs the least in the total communication. The coefficients of nl and n are both less than the other two schemes [31, 33]. The concrete lower rates are 59.9% and 33% than [33] for nl and n, and 31.6% and 48.5% than [31]. Besides, to give an intuitive comparison, we list the total communication cost of three schemes in Figure 6, where we set $n = l = 40$. From the figure, we can see clearly that our scheme is most effective one in communication cost aspect.

VIII. Conclusion

Mobile edge computing is a new paradigm that complements the could computing and IoT complement to each other. This paper defined the privacy preserving data aggregation for mobile edge computing assisted IoT applications, which not only save the communication overhead of the full system, but also preserve privacy of terminal devices. Hereafter, we designed a privacy preserving data aggregation for mobile edge computing assisted IoT applications based on the homomorphic property of Boneh-Goh-Nissim cryptosystem. The proposed scheme can protect privacy and provide source authentication and integrity. The performance analysis show that the proposed scheme can save almost half of the communication cost compared with traditional method. Therefore, it is very suitable for the mobile edge computing assisted IoT applications. In future work, we will evaluate the proposed scheme under realistic IoT environment. Besides, the mobile edge computing is a new thing, and the research on its security and privacy issues is just getting started. Futhermore, the characteristics of mobile edge computing, such as multi-source heterogeneity, cross-trust domain, and limited terminal resources, may create new security and privacy issues, and the traditional security and privacy preserving mechanisms of cloud computing may not suitable for mobile edge computing. In future research, we will also focus on the lightweight authentication mechanisms across trust domains and the data sharing schemes with privacy protection in different trust domains suitable for mobile edge computing.

References

[1] M. Peter and T. Grance, "The nist definition of cloud computing," 2011.

[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of The ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[4] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, 2014.

[5] R. Want, "An introduction to rfid technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[7] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: A survey," *Future Generation Computer Systems*, vol. 56, pp. 684–700, 2016.

[8] M. Diaz, C. Martin, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing," *Journal of Network and Computer Applications*, vol. 67, pp. 99–117, 2016.

[9] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, and K. R. Choo, "A robust and energy efficient authentication protocol for industrial internet of things," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1606–1615, 2018.

[10] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, "A robust ecc-based provable secure authentication protocol with privacy preserving for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3599–3609, 2018.

[11] A. Nordrum, "The internet of fewer things [news]," *IEEE Spectrum*, vol. 53, no. 10, pp. 12–13, 2016.

[12] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted internet of things," *IEEE Cloud Computing*, vol. 4, no. 1, pp. 34–42, 2017.

[13] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computingła key technology towards 5g," *ETSI white paper*, vol. 11, no. 11, pp. 1–16, 2015.

[14] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[15] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, 2018.

[16] S. Yi, Z. Hao, Z. Qin, and Q. Li, "Fog computing: Platform and applications," in *In 2015 Third IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. IEEE, 2015, pp. 73–78.

[17] K. Ha, Z. Chen, W. Hu, W. Richter, P. Pillai, and M. Satyanarayanan, "Towards wearable cognitive assistance," pp. 68–81, 2014.

[18] B. Chun, S. Ihm, P. Maniatis, M. Naik, and A. Patti, "Clonecloud: elastic execution between mobile device and cloud," pp. 301–314, 2011.

[19] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K. R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Computer Networks*, vol. 129, pp. 429–443, 2017.

[20] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016.

[21] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, no. 1, pp. 680–698, 2018.

[22] D. Boneh, E.-J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts," in *Theory of Cryptography Conference*. Springer, 2005, pp. 325–341.
[23] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 4, pp. 681–694, 2014.
[24] K. Shim and C. Park, "A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 8, pp. 2128–2139, 2015.
[25] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient id-based aggregate signature scheme for wireless sensor networks," *IEEE Internet of Things Journal*, vol. 4, no. 2, pp. 546–554, 2017.
[26] 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.
[27] 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, 2014.
[28] H. Jin, L. Su, H. Xiao, and K. Nahrstedt, "Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc' 16)*, 2016, pp. 341–350.
[29] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.
[30] C. Fan, S. Huang, and Y. Lai, "Privacy-enhanced data aggregation scheme against internal attackers in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 1, pp. 666–675, 2014.
[31] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Inform*, vol. 13, pp. 2428–2435, 2017.
[32] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *theory and application of cryptographic techniques*, pp. 223–238, 1999.
[33] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Generation Computer Systems*, vol. 78, pp. 712 – 719, 2018.
[34] G. Castagnos and F. Laguillaumie, "Linearly homomorphic encryption from DDH," in *In Cryptographers' Track at the RSA Conference*, 2015, pp. 487–505.
[35] X. Sun and N. Ansari, "Edgeiot: Mobile edge computing for the internet of things," *IEEE Communications Magazine*, vol. 54, no. 12, pp. 22–29, 2016.
[36] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," 1997.
[37] F. Wu, X. Li, L. Xu, A. K. Sangaiah, and J. J. Rodrigues, "Authentication protocol for distributed cloud computing," *IEEE Consumer Electronics Magazine*, 2018.

Xiong Li received the Ph.D. degree in computer science and technology from the Beijing University of Posts and Telecommunications, Beijing, China, in 2012. He is currently an Associate Professor with the School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, China. He has authored over 100 referred papers. His current research interests include cryptography and information security. He was a recipient of the 2015 Journal of Network and Computer Applications Best Research Paper Award.

Shanpeng Liu is currently a M.S. candidate of Hunan University of Science and Technology, China. His research interests include cloud computing security and security protocols.

Fan Wu received the ME degree in computer software and theory from Xiamen University, Xiamen, China, in 2008. Now, he is an Associate Professor in Xiamen Institute of Technology. His current research interests include information security, internet protocols, and network management.

Saru Kumari received the Ph.D. degree in mathematics from Chaudhary Charan Singh University, Meerut, India, in 2012. She is currently an Assistant Professor in the Department of Mathematics, Chaudhary Charan Singh University. Her current research interests include information security, digital authentication, and applied mathematics.

Joel J.P.C. Rodrigues (S01, M06, SM06) is a professor and senior researcher at the National Institute of Telecommunications (Inatel), Brazil and senior researcher at the Instituto de Telecomunicações, Portugal. Prof. Joel is the leader of the Internet of Things Research Group (Inatel), Director for Conference Development-IEEE ComSoc Board of Governors, and IEEE Distinguished Lecturer. He has authored or coauthored over 650 papers in refereed international journals and conferences, 3 books, and 2 patents. He had been awarded several Outstanding Leadership and Outstanding Service Awards by IEEE Communications Society and several best papers awards.