Received April 3, 2020, accepted April 13, 2020, date of publication April 15, 2020, date of current version April 30, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987749

Privacy and Energy Co-Aware Data Aggregation Computation Offloading for Fog-Assisted IoT Networks

SIGUANG CHEN[1,2], (Member, IEEE), ZIHUI YOU[1], AND XIUKAI RUAN[3]

[1]Jiangsu Engineering Research Center of Communication and Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[2]Anhui Provincial Key Laboratory of Network and Information Security, Anhui Normal University, Wuhu 241000, China
[3]Institute of Intelligent Locks, Wenzhou University, Wenzhou 325035, China

Corresponding author: Xiukai Ruan (ruanxiukai@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61971235, Grant 61771258, and Grant 61671329, in part by the Six Talented Eminence Foundation of Jiangsu province under Grant XYDXXJS-044, in part by the 333 High-level Talents Training Project of Jiangsu province, in part by the 1311 Talents Plan of NUPT, in part by the China Postdoctoral Science Foundation under Grant 2018M630590, in part by the Scientific Research Foundation of NUPT under Grant NY217057 and Grant NY218058, in part by the Open Research Fund of Anhui Provincial Key Laboratory of Network and Information Security under Grant AHNIS2020001, in part by the CERNET Innovation Project under Grant NGII20190702, and in part by the Open Research Fund of Jiangsu Engineering Research Center of Communication and Network Technology, NUPT, under Grant JSGCZX17011.

ABSTRACT With the exponential growth of the data generated by Internet of Things (IoT) devices, computation offloading becomes a promising method to alleviate the computation burden of local IoT device and improve processing latency. In order to address the bottleneck problem of limited resources in IoT device more efficiently and provide security guarantee in data processing and forwarding process, in this paper, we propose a privacy and energy co-aware data aggregation computation offloading for fog-assisted IoT networks. Specifically, a fog-assisted three-layer security computing architecture is developed to counteract security threats and enable the aggregation operation can be performed in ciphertext. Meanwhile, a momentum gradient descent based energy-efficient offloading decision algorithm is developed to minimize the total energy consumption of computation tasks, which can achieve the optimal value with fast convergence rate. Finally, the security and performance evaluations reveal that the developed data aggregation offloading scheme is a secure data processing scheme and achieves significant performance advantage in energy consumption. For example, the total energy consumption can be reduced by an average of 23.1% compared with benchmark PGCO solution.

INDEX TERMS Computation offloading, fog computing, data aggregation, data security.

I. INTRODUCTION

Internet of Things (IoT), as an important force to promote the development of the information industry, has penetrated into people's lives. With the continuous growth of the number of devices connected to the network, the data generated by IoT devices show an explosive growth trend [1]. In these large scale data, they usually include a large number of sensitive data containing users' private information. Therefore, how to deal with mass data efficiently with privacy preservation has become an urgent problem that needs to be solved. At the same time, many IoT applications have real-time service requirements, which will lead to disastrous effects if the response delay exceeds the tolerable latency. In addition, energy consumption is also an important metric that needs to be considered, it will affect the network efficiency and lifetime significantly. Consequently, how to improve the processing efficiency of large amounts of data with security guarantee has become a huge challenge.

Under the scenario of massive data need to be processed, cloud computing emerges as the times require, which can effectively handle the different tasks of various devices. However, as the number of smart devices increases, bandwidth consumption and data processing burdens become heavier and heavier, task processing will face various problems, such as high delay, congestion, energy consumption and security

The associate editor coordinating the review of this manuscript and approving it for publication was Nan Cheng.

risk. Fortunately, the emergence of fog computing [2]–[4] effectively overcomes these shortcomings of cloud computing. Fog computing paradigm is closer to the terminal device with low data processing delay and strong mobility, which can effectively reduce core network pressure and save energy. These advantages make that fog computing can be applied in many fields, such as industrial IoT (IIoT) [5], [6], vehicular network [7], healthcare [8] and smart grid [9]. Furthermore, in order to enhance task processing efficiency and alleviate resource constraint problem of single edge device, the computation offloading theory was studied. Fog computing-based computation offloading emerges as a promising solution to address above challenge (i.e., the processing efficiency problem of big data).

At present, the research schemes of computation offloading mainly focus on optimizing offloading ratio to minimize the global energy consumption or time delay. For example, He *et al.* [10] proposed a delay-aware energy efficient computation offloading scheme for fog radio access networks (F-RANs) with hybrid energy supplies, it can minimize the consumption of non-renewable grid energy under delay constraint. From time delay perspective, Yousefpour *et al.* [11] conceived a delay-minimizing collaboration and offloading policy that aims to reduce the service delay of IoT applications. Similarly, in [12], the authors constructed an analytical framework of fair task offloading for fog computing networks, which offloads tasks to the selected nodes based on a rule that minimizes the task delay. In [13], Wang *et al.* developed a completion time minimization offloading mechanism with joint optimization of computation resource and offloading decision for fog-enabled IoT. Unfortunately, they lack the security consideration to guarantee data security that is important for users' privacy data.

In fog/edge computing scenario, jointly considering the privacy preservation of big data and system performance has become a trend [14]–[16]. For the sake of ensuring data security and reducing energy consumption (or time delay), many privacy preservation based data offloading schemes were investigated. For example, Wang *et al.* [17] developed a lightweight anonymous mutual authentication scheme for n-times computation offloading in IoT, it can resist several security threats with low latency, such as compromising attack, privacy leaking and denial of service (DoS) attack. In [18], Tang *et al.* proposed a blockchain-based offloading approach, it can verify each fog server's authenticity and security, and then constantly maintain a set of candidate authorized fog servers by leveraging blockchain technology. What's more, the offloading decision can be made in a real-time fashion and satisfy the demand for computation resource in mobile applications. From the intelligent decision perspective, in [19], Min *et al.* proposed a reinforcement learning-based privacy preserving smart offloading mechanism, it can provide the privacy preservation for healthcare users and reduce the processing latency and energy consumption of sensing device. Indeed, these schemes improve the security of data processing on the basis of optimizing energy consumption or time delay. However, they ignore the possibility of specific data manipulation on the ciphertext, which actually limits further improvement of network performance. For example, if the data aggregation technology can be introduced to aggregate ciphertext, the network performance will be improved significantly.

In order to overcome shortcomings of the current research schemes, i.e., to further enhance network performance with privacy protection, from the joint consideration perspective of privacy preservation, data aggregation operation and offloading decision, this paper proposes a privacy and energy co-aware data aggregation computation offloading for fog-assisted IoT networks. The major contributions are expressed as follows.

- First, we construct a fog-assisted three-layer security computing architecture, in which a privacy-aware data processing mechanism is developed to counteract eavesdropping and compromising attacks and enable the aggregation operation can be performed on ciphertext.
- The second is that an energy-aware computation offloading optimization problem is formulated to minimize the total energy consumption of computation tasks, and a momentum gradient descent based energy-efficient offloading decision algorithm is proposed to address such problem. This solving algorithm can achieve the optimal value with fast convergence rate for the momentum gradient updates the downward direction by considering the momentum accumulated in the previous iteration in conjunction with the current gradient direction.
- Finally, the security and performance analyses verify that the developed data aggregation computation offloading scheme is a secure data processing scheme and achieve a significant reduction in energy consumption with faster convergence rate.

The remainder of this paper is arranged as follows. Briefly, Section II presents related works on our research topic. The system model is constructed and expounded in Section III. In Section IV, the proposed offloading scheme is illustrated in detail. Whereafter, the numerical results are given in Section V. Finally, we make a concise conclusion in Section VI.

II. RELATED WORK

With the advent of big data era, data present an explosive growth trend. The mismatch between the limited computing resource of sensing device and intensive real-time computing tasks leads to the problem of excessive energy consumption and poor service quality. Around these thorny issues, the computation offloading technology has become a hotspot in recent years due to its advantages of timeliness and energy saving. For example, Chang *et al.* [20] proposed an energy efficient computation offloading scheme in a multi-user fog computing system, which minimizes the energy consumption with execution delay constraint. Similarly, in order to balance the response time and energy consumption for multiple fog devices with multiple running applications, in [21], Jiang *et al.* presented an energy-efficient offloading decision mechanism and offloading dispatcher to dispatch applications to the corresponding devices by effectively managing the computation and communication resources of all devices in fog computing architecture. Based on the trade-off between the considered computation and communication costs, in work [22], a revenue maximization problem was formulated to distribute the data among fog nodes. Based on fog-to-fog collaboration consideration, Al-khafajiy *et al.* [23], [24] investigated fog computing performance improvement scheme by integrating the load balance and computation capability sharing among fog nodes. From the intelligent decision perspective, Ali *et al.* [25] designed a deep learning-based energy-efficient computation offloading method, it achieves optimal offloading decision with performance improvement by comprehensively considering energy, delay, task load and network condition. Although the above schemes can effectively improve the performance gains in terms of latency and energy consumption, the security of data transmitting and processing is not considered in their network scenario, which is important for several sensitive privacy data.

In order to effectively solve the data security problem and reduce communication overhead, in recent years, data aggregation involving privacy protection has become a research focus in IoT. For instance, Huo *et al.* [26] developed a real-time stream data aggregation framework with adaptive ω-event differential privacy which can ensure data security over infinite stream. Okay and Ozdemir [27] presented a novel Domingo-Ferrer additive privacy based secure data aggregation scheme for fog computing-assisted smart grids, it can achieve end-to-end confidentiality while ensuring the low communication and storage overhead. Similarly, Lyu *et al.* [9] investigated an efficient and privacy-preserving aggregation system with the aid of fog computing architecture, it can minimize the privacy leakage and mitigate the utility loss. In work [28], a device-oriented anonymous privacy-preserving scheme was constructed to efficiently preserve the privacy of sensitive data in the fog-enhanced IoT environment.

Furthermore, for the sake of reducing service latency and energy consumption with security guarantee, the integration of privacy protection and computation offloading attracts great attention. For example, in [29], a privacy-aware data offloading method in edge computing was proposed to prohibit privacy leakage and achieve low latency. Similarly, He *et al.* [30] developed a constrained Markov decision process based privacy-aware task offloading scheduling algorithm, which achieves the best possible delay and energy consumption with a high level of privacy. To solve the risk of disclosing possibly sensitive user data to eavesdroppers, He *et al.* [31] studied a novel physical-layer assisted privacy-preserving offloading scheme, in which the edge server proactively broadcasts jamming signals to impede eavesdropping attack and leverages full-duplex communication technique to effectively suppress the self-interference. In work [32], an energy-efficient computation offloading method with privacy preservation, was proposed to improve the load balance and energy consumption of all the edge nodes in edge computing-enabled 5G networks. Although these works perform well in terms of energy consumption and data security, there is still room for improvement in system performance. For example, if the specific computation operation (such as data aggregation) can be integrated into the existing scheme, the data processing and energy efficiencies of above offloading schemes can be improved significantly.

III. NETWORK MODEL

In this section, as displayed in Fig. 1, we construct a fog-assisted secure three-layer computing model for IoT. From bottom to the top, are respectively defined as the sensing layer, the fog layer and the cloud layer, and the data is processed layer by layer. The whole coverage area of IoT is divided into multiple sub-areas, each of them contains a fog node and several IoT sensing devices. We define that there exists n IoT sensing devices in one sub-area. The specific functions of these layers and threat model are defined in the following part.

A. SENSING LAYER

This layer is composed of IoT sensing devices, which are deployed to the corresponding places for data sensing. We assume that each IoT device needs to calculate the average value of the generated data in a time period t_j, where j represents the index of the time period, and the length of each time period is a constant T. We assume that each device generates data at a fixed rate, and these data are all integer and greater than zero. What's more, the different devices generate data at different speeds. We take a sub-area as an example, first, to ensure the security of data processing, the data generated by the n devices in the different time periods are encrypted by Paillier encryption. Next, the sensing layer will make appropriate offloading decision to solve the resource constraint problem of sensing device by choosing the most suitable task offloading ratio α_i. We define $L_i^{t_j}$ (Mb) as the task size of device i during the time period t_j. The system tends to offload the partial task $\alpha_i \cdot L_i^{t_j}$ to the nearby fog node and processes the remaining task locally. The result of the local computation part of device i in the time period t_j is denoted as $a_i^{t_j}$ and the sensing layer will transmit the computation result to the cloud layer.

B. FOG LAYER

This layer is the intermediate layer between the sensing layer and the cloud layer, which is deployed at the edge of the network. Each sub-area contains a fog node which is able to interact with IoT devices within its coverage area. Compared with IoT devices, fog node has stronger computation capability. Based on the offloading decision, the fog node accepts the computation task $\alpha_i \cdot L_i^{t_j}$ that transmitted to it by

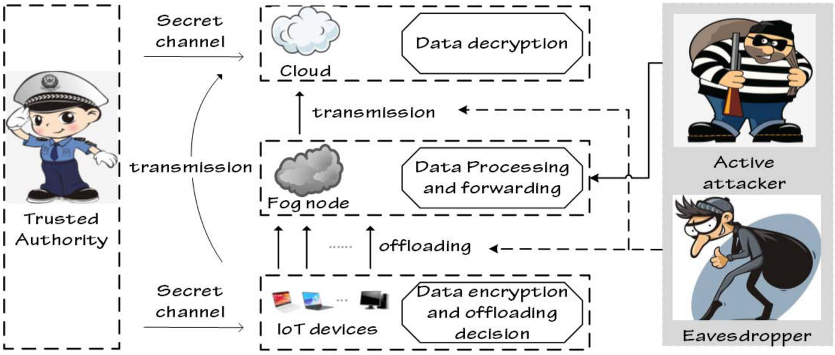

FIGURE 1. Fog-assisted three-layer computing architecture for IoT.

device in its coverage region. Next, the fog node will perform the aggregation operation on the received computation task $\alpha_i \cdot L_i^{tj}$, and the aggregation result can be denoted as b_i^{tj}. Finally, this layer will transmit the computation result to the cloud layer.

C. CLOUD LAYER

The cloud layer receives the computation results from the sensing layer and the fog layer. This layer calculates the final result c_i^{tj} by performing the aggregation operation on a_i^{tj} and b_i^{tj}. At the same time, the cloud layer utilizes the private key which is assigned to it by the trusted authority to decrypt the aggregated encrypted data, i.e., to get data sum of each IoT device during each time period. Finally, the sum is divided by the number of data generated by each device in the corresponding time period to get the required average value.

D. TRUSTED AUTHORITY

We assume that there exists a trusted third party, which has strong processing ability, is mainly responsible for generating the key and distributing it to the corresponding entity.

E. ADVERSARY MODEL

Based on the defined system model, we mainly consider the following two types of security threats, i.e., the eavesdropping and compromising attacks.

1) EAVESDROPPING ATTACK

The eavesdropper can eavesdrop all communication links and obtain the transmitted data, so it can obtain the user's private information. As a result, whether the data transmitted from the sensing layer to the fog layer or the data from the fog layer to the cloud layer, the system must ensure that the data are transmitted in the ciphertext form. It can guarantee the privacy of user's data for the eavesdropper is unable to accurately restore the data even if it successfully observes the data over the data link.

2) COMPROMISING ATTACK

We assume that the active attacker has enough resources to compromise the fog node, so the data of the fog node will be exposed to the attacker. The system must ensure that the data of the fog node are always processed or stored in the ciphertext form, so as to ensure the security of user's data even if the attacker obtains the data of fog node.

Important notations used in this paper are given in the following TABLE 1.

IV. PRIVACY AND ENERGY CO-AWARE COMPUTATION OFFLOADING MECHANISM

In this section, we propose a privacy and energy co-aware computation offloading mechanism for fog-assisted IoT

TABLE 1. Notation definitions.

Notation	Definition
$L_i^{t_j}$	Task size of device *i* during the time period t_j
α_i	Task offloading ratio of device *i*
$a_i^{t_j}, b_i^{t_j}, c_i^{t_j}$	The aggregation result of device *i*'s task in the local/fog/cloud during the time period t_j
$D_i\left(t_j\right), D_i'\left(t_j\right)$	The data generated by the device *i* in the time period t_j/the ciphertext of $D_i\left(t_j\right)$
sk, *pk*	The private key/public key
$D'_{i\_offload}\left(t_j\right)$, $D'_{i\_local}\left(t_j\right)$	The partial ciphertext of $D_i\left(t_j\right)$ that are offloaded to the fog node/the remaining ciphertext that are processed in local
M	The final decryption result at cloud
β_i	The occupation ratio of fog node's computation capacity assigned to device *i*
R_i	The data transmission rate of device *i*
U_d^{comp}, U_f^{comp}	The computation capacity of device/fog node
P_d^{comp}, P_f^{comp}, $P_{d_i}^{comp}$	The computation power of device/the computation power of fog node/the transmission power of device *i*
$E_{d_i}^{comp}, E_f^{comp}$, $E_{d_i}^{tran}$	The local computation energy consumption of device *i*/the computation energy consumption of fog node/the transmission energy consumption of device *i*
E_{total}	The total energy consumption
J	The energy consumption of device *i*
$o_i(k)$,$q_i(k)$,$r_i(k)$	The accumulated momentum of α_i/ β_i/R_i at iteration *k*

networks, the purpose is to minimize the total energy consumption with privacy preservation. The detailed encryption, offloading and decryption processes are explained as follow.

A. PRIVACY-AWARE DATA PROCESSING

1) DATA ENCRYPTION AND OFFLOADING AT IOT DEVICE

Based on the definition of network model, the data generated by the device i in the time period t_j can be represented as

$$D_i\left(t_j\right) = \left[D_{i1}\left(t_j\right), D_{i2}\left(t_j\right) \ldots D_{iz_i}\left(t_j\right)\right], \tag{1}$$

where Z_i represents the number of data generated by the device i in the time period t_j.

All the data generated by the device i in the time period t_j are encrypted by the Paillier encryption, operation steps are shown as follows.

We assume that p and q are two large prime numbers which satisfies

$$\gcd(pq, (p-1)(q-1)) = 1, \tag{2}$$

we define that $N = pq$, then we select a generated element $g \in Z^*_{n^2}$, it can be denoted as

$$\gcd\left(L\left(g^{\lambda} \bmod N^2\right), N\right) = 1, \tag{3}$$

where

$$L(u) = (u-1)/N. \tag{4}$$

The private key can be expressed as

$$sk = \lambda(N) = lcm(p-1, q-1), \tag{5}$$

and the public key can be represented as

$$pk = (N, g), \tag{6}$$

where the private key is assigned to the cloud by the trusted authority, and the public key is assigned to the sensing devices by the trusted authority.

The generated data are encrypted in the sensing layer. For any plaintext $m \in D_i\left(t_j\right)$, we select $r \in Z^*_n$ at random to get the corresponding ciphertext, which can be denoted as

$$c = E_{pk}(m) = g^m r^N \bmod N^2. \tag{7}$$

According to the formula (1), the set of ciphertext can be shown as

$$D'_i\left(t_j\right) = \left[D'_{i1}\left(t_j\right), D'_{i2}\left(t_j\right) \ldots D'_{iz_i}\left(t_j\right)\right]. \tag{8}$$

Based on the offloading decision, the part of ciphertext which are offloaded to the fog node can be written as

$$D'_{i\_offload}\left(t_j\right) = \left[D'_{i1}\left(t_j\right), D'_{i2}\left(t_j\right) \ldots D'_{i\alpha_i Z_i}\left(t_j\right)\right], \tag{9}$$

where the remaining ciphertext to be processed locally can be given as

$$D'_{i\_local}\left(t_j\right) = [D'_{i(\alpha_i z_i+1)}(t_j), D'_{i(\alpha_i z_i+2)}(t_j) \ldots D'_{iz_i}(t_j)]. \tag{10}$$

2) DATA AGGREGATION

We make use of the additive homomorphism property of Paillier encryption during the data aggregation, the local aggregation ciphertext of device i during time period t_j can be defined as

$$a_i^{t_j} = \prod_{k=\alpha_i z_i+1}^{z_i} D'_{ik}\left(t_j\right) \bmod N^2, \tag{11}$$

and the offloaded aggregation ciphertext can be written as

$$b_i^{t_j} = \prod_{k=1}^{\alpha_i z_i} D'_{ik}\left(t_j\right) \bmod N^2. \tag{12}$$

Next, the cloud layer receives the aggregation results respectively from the sensing and fog layer, and conducts secondary aggregation on them to obtain the final aggregation result, which can be organized as

$$\begin{aligned} c_i^{t_j} &= \prod_{k=1}^{Z_i} D'_{ik}\left(t_j\right) \bmod N^2 \\ &= \prod_{k=1}^{z_i} g^{D_{ik}(t_j)} r_k^N \bmod N^2 \\ &= \left(g^{D_{i1}(t_j)} \cdot g^{D_{i2}(t_j)} \ldots g^{D_{iZ_i}(t_j)} \bmod N^2\right) \\ &\quad \cdot \left(\prod_{k=1}^{z_i} r_k\right)^N \bmod N^2 \\ &= g^{D_{i1}(t_j)+D_{i2}(t_j)+\cdots D_{iZ_i}(t_j)} \left(\prod_{k=1}^{z_i} r_k\right)^N \bmod N^2. \end{aligned} \tag{13}$$

In order to show $c_i^{t_j}$ more intuitive and in a Paillier encrypted form. We define the following two variables

$$M = D_{i1}\left(t_j\right) + D_{i2}\left(t_j\right) + \ldots + D_{iz_i}\left(t_j\right), \tag{14}$$

$$R = \prod_{k=1}^{z_i} r_k. \tag{15}$$

Finally, the aggregation ciphertext can be reformulated into the following format, and which is in according with the ciphertext form of Paillier encryption.

$$c_i^{t_j} = g^M R^N \bmod N^2. \tag{16}$$

3) DATA DECRYPTION AT CLOUD

As mentioned above, after receiving the final calculation result $c_i^{t_j}$, the cloud layer immediately performs decryption operation on it. We denote the final decryption result as M, the specific decryption process is shown as

$$\begin{aligned} M &= D_{sk}\left(c_i^{t_j}\right) \\ &= \left(L\left(c^{\lambda(N)} \bmod N^2\right)/L\left(g^{\lambda(N)} \bmod N^2\right)\right) \bmod N. \end{aligned} \tag{17}$$

B. ENERGY-AWARE COMPUTATION OFFLOADING OPTIMIZATION

On the premise of ensuring the security of data processing, this subsection formulates an energy-aware computation offloading optimization problem which is aimed at minimizing the total energy consumption during the data processing.

In our network model, we assume that the task of each device is to calculate the average value of the data generated by itself during the time period t_j. Let α_i, R_i respectively represent the task offloading ratio and the data transmission rate of device i, and let β_i represent the occupation ratio of fog node's computation capacity assigned to device i. We define $L_i^{t_j}$ (Mb) as the task size of device i during the time period t_j. We assume that all the devices in the sub-area have the same computation capacity and power, which are respectively defined as U_d^{comp} (Mb/s) and P_d^{comp} (W). Besides, the computation capacity and power of fog node are respectively defined as U_f^{comp} (Mb/s) and P_f^{comp} (W), and the transmission power of device i is defined as $P_{d_i}^{tran}$ (W). All the devices in the sub-area share a wireless channel, and the channel is equally allocated to these devices for the data transmission operations.

Transmission power of the device *i*: According to Shannon equation, the transmission rate of the device i can be expressed as

$$R_i = \frac{B}{n}\log_2\left(1+\frac{n\cdot P_{d_i}^{tran}\cdot h_i^2}{N_0 B}\right), \tag{18}$$

where B represents the wireless channel bandwidth, $P_{d_i}^{tran}$ represents the transmission power of the device i, h_i represents the channel gain of the device i, and N_0 represents the white Gaussian noise. Then the transmission power of the device i can be expressed as

$$P_{d_i}^{tran} = \frac{N_0 B}{n\cdot h_i^2}\left(2^{\frac{n\cdot R_i}{B}}-1\right). \tag{19}$$

Energy consumption: We assume that the local computation energy consumption of device i, the computation energy consumption of fog node and the transmission energy consumption of device i can be respectively represented as $E_{d_i}^{comp}$, E_f^{comp} and $E_{d_i}^{tran}$, the specific expressions of the above three energy consumptions are respectively given as

$$E_{d_i}^{comp} = P_{d_i}^{comp}\cdot\frac{(1-\alpha_i)\,L_i^{t_j}}{U_{d_i}^{comp}}, \tag{20}$$

$$E_f^{comp} = P_f^{comp}\cdot\frac{\alpha_i\cdot L_i^{t_j}}{\beta_i\cdot U_f^{comp}}, \tag{21}$$

$$E_{d_i}^{tran} = \frac{N_0 B}{n\cdot h_i^2}\left(2^{\frac{n\cdot R_i}{B}}-1\right)\cdot\frac{n\cdot\alpha_i\cdot L_i^{t_j}}{B}. \tag{22}$$

The total energy consumption E_{total} contains the computation energy consumption of local IoT devices, the transmission energy consumption of IoT devices and the computation energy consumption of fog node, which can be expressed as

$$\begin{aligned} E_{total} &= \sum_{i=1}^{n}\left(E_{d_i}^{comp}+E_{d_i}^{tran}+E_f^{comp}\right)\\ &= \sum_{i=1}^{n}\left(P_{d_i}^{comp}\cdot\frac{(1-\alpha_i)\,L_i^{t_j}}{U_{d_i}^{comp}}\right.\\ &\quad+\frac{N_0 B}{n\cdot h_i^2}\left(2^{\frac{n\cdot R_i}{B}}-1\right)\cdot\frac{n\cdot\alpha_i\cdot L_i^{t_j}}{B}\\ &\quad\left.+P_f^{comp}\cdot\frac{\alpha_i\cdot L_i^{t_j}}{\beta_i\cdot U_f^{comp}}\right). \end{aligned} \tag{23}$$

Here we formulate an optimization problem, the objective of which is to minimize the total energy consumption E_{total} by adjusting the parameters α_i, R_i and β_i, and the specific optimization problem can be written as

$$P1:\ \min_{\alpha_i,\beta_i,R_i} E_{total} \tag{24}$$

$$\begin{aligned} s.t.\quad T_{i,total} &= \max\left[T_{i,local},T_{i,offloaded}\right]\le T, &&\text{(24a)}\\ 0 &\le \alpha_i\le 1, &&\text{(24b)}\\ \sum_{i=1}^{n}\beta_i &\le 1, &&\text{(24c)}\\ \sum_{i=1}^{n}R_i &\le B, &&\text{(24d)}\\ 0 &< \beta_i\le 1. &&\text{(24e)} \end{aligned}$$

In objective function (24), the purpose is to minimize the total energy consumption E_{total} by adjusting the parameters α_i, R_i and β_i. Constraint (24a) ensures that the maximum delay of the device i to complete the task can't exceed the time period. Constraint (24b) indicates the offloading ratio of device i should be between 0 and 1. Constraint (24c) ensures that the sum of the occupation ratio of fog node's computation capacity assigned to each device does not exceed the unity. Constraint (24d) ensures that the sum of the data transmission rate of each device does not exceed the value of channel bandwidth. Constraint (24e) indicates the occupation ratio of fog node's computation capacity assigned to each device should be greater than 0 and less than or equal to 1, i.e., once the local device offloads the computation task to the fog node, this task will be assigned certain computation resource from fog node.

C. OPTIMIZATION SOLUTION

In this subsection, in order to solve the optimization problem P1, we develop a momentum gradient descent based energy-efficient offloading decision algorithm for achieving the minimum energy consumption.

First, we define function J to represent the energy consumption of device i's computation task, which can be expressed as

$$J = P_d^{comp} \cdot \frac{(1-\alpha_i)\, L_i^{tj}}{U_d^{comp}} + \frac{N_0 B}{n \cdot h_i^2}\left(2^{\frac{n \cdot R_i}{B}} - 1\right) \cdot \frac{n \cdot \alpha_i \cdot L_i^{tj}}{B} + P_f^{comp} \cdot \frac{\alpha_i \cdot L_i^{tj}}{\beta_i \cdot U_f^{comp}}. \tag{25}$$

Then, by means of partial derivative calculation, the gradient of the function J with respect to α_i, β_i and R_i can be respectively represented as $\frac{\partial J}{\partial \alpha_i}$, $\frac{\partial J}{\partial \beta_i}$ and $\frac{\partial J}{\partial R_i}$, the specific definitions are shown as follows:

$$\frac{\partial J}{\partial \alpha_i} = -\frac{P_{d_i}^{comp} \cdot L_i^{tj}}{U_{d_i}^{comp}} + \frac{N_0 \cdot L_i^{tj}}{h_i^2} \cdot 2^{\frac{n \cdot R_i}{B}} - \frac{N_0 \cdot L_i^{tj}}{h_i^2} + \frac{L_i^{tj} \cdot P_f^{comp}}{U_f^{comp}} \cdot \frac{1}{\beta_i}, \tag{26}$$

$$\frac{\partial J}{\partial \beta_i} = -\frac{L_i^{tj} \cdot P_f^{comp} \cdot \alpha_i}{U_f^{comp} \cdot \beta_i^2}, \tag{27}$$

$$\frac{\partial J}{\partial R_i} = \frac{\ln 2 \cdot N_0 \cdot L_i^{tj} \cdot n \cdot \alpha_i}{h_i^2 \cdot B} \cdot 2^{\frac{n \cdot R_i}{B}}. \tag{28}$$

Next, we can leverage the gradient descent with momentum method to update variables α_i, β_i and R_i, which are shown as

$$\begin{cases} \alpha_i(k+1) = \alpha_i(k) - o_i(k+1), \\ \beta_i(k+1) = \beta_i(k) - q_i(k+1), \\ R_i(k+1) = R_i(k) - r_i(k+1), \end{cases} \tag{29}$$

where

$$\begin{cases} o_i(k+1) = \gamma \cdot o_i(k) + s \cdot g_i(k), \\ q_i(k+1) = \gamma \cdot q_i(k) + s \cdot g_i(k), \\ r_i(k+1) = \gamma \cdot r_i(k) + s \cdot g_i(k), \end{cases} \tag{30}$$

where symbols $k, s, \gamma, g_i(k)$ respectively represent the number of iterations, the step size of iteration, the attenuation value and the gradient of the function J. And variables $o_i(k)$, $q_i(k)$ and $r_i(k)$ respectively represent the accumulated momentum of α_i, β_i and R_i at their iterative processes. The specific expression of $g_i(k)$ is written as

$$g_i(k) = \begin{cases} \dfrac{\partial J(k)}{\partial \alpha_i(k)}, \\ \dfrac{\partial J(k)}{\partial \beta_i(k)}, \\ \dfrac{\partial J(k)}{\partial R_i(k)}. \end{cases} \tag{31}$$

When the stop condition is reached (i.e., reaching the maximum number of iterations), the iteration for α_i, β_i and R_i will stop, and the optimal value of them will be achieved. Meanwhile, the minimum energy consumption E_{total}^* can also be obtained, which can be expressed as

$$E_{total}^* = \sum_{i=1}^{n}\left(\frac{P_d^{comp} \cdot L_i^{tj}}{U_d^{comp}} - \frac{P_d^{comp} \cdot L_i^{tj} \cdot \alpha_i^*}{U_d^{comp}} + \frac{N_0 \cdot L_i^{tj} \cdot \alpha_i^*}{h_i^2} \cdot 2^{\frac{n \cdot R_i^*}{B}} - \frac{N_0 \cdot L_i^{tj} \cdot \alpha_i^*}{h_i^2} + \frac{L_i^{tj} \cdot P_f^{comp}}{U_f^{comp}} \cdot \frac{\alpha_i^*}{\beta_i^*}\right), \tag{32}$$

where α_i^* represents the optimal offloading ratio of device i, R_i^* represents the optimal data transmission rate of device i, and β_i^* represents the optimal occupation ratio of fog node's computation capacity assigned to device i.

To facilitate the understanding, the detailed solution process of the minimum energy consumption can be found in Algorithm 1.

Algorithm 1 Momentum Gradient Descent Based Energy-Efficient Offloading Decision Algorithm

```
Input:
    The task size $L_i^{tj}$, bandwidth $B$, time period $T$, step size $s$,
    and attenuation value $\gamma$.
Output:
    The optimal values $\alpha_i^*$, $\beta_i^*$, $R_i^*$ and $E_{total}^*$.
begin
Initializing $\alpha_i$, $\beta_i$, $R_i$ and setting $k$ =1;
while constraint conditions (24a)-(24e) are all satisfied; do
    Updating the $\alpha_i(k)$, $\beta_i(k)$ and $R_i(k)$ by formula (29)
    with momentum (30) and gradient function (31);
    $k = k + 1$;
end while
Obtaining the optimal values $\alpha_i^*$, $\beta_i^*$ and $R_i^*$;
The optimal energy consumption $E_{total}^*$ can be obtained
by calculating equation (32) with the optimal ($\alpha_i^*$, $\beta_i^*$, $R_i^*$).
end
```

V. SECURITY AND PERFORMANCE EVALUATION

In this section, theoretical analysis and numerical results are used to verify the security and performance advantages of our proposed privacy and energy co-aware computation offloading mechanism.

A. SECURITY EVALUATION

1) SECURITY ANALYSIS

Eavesdropping attack: The first type of possible attack is called eavesdropping attack, in which an attacker might eavesdrop communication links to obtain the transmitted data. To effectively defend against such attack, this paper utilizes the Paillier algorithm to encrypt the data generated by the IoT devices, the encrypted form of which can be represented as $c = E_{pk}(m) = g^m r^N \mod N^2$. Even if the eavesdropper successfully eavesdrops the transmitted data in the communication links, they can only obtain the corresponding ciphertext and cannot obtain the correct plaintext for without the corresponding decryption key. The specific reason is that the data encrypted by Paillier algorithm has semantic security from the chosen plaintext attack [33]. Therefore, the proposed scheme can effectively protect users' privacy during the transmission of the links.

Compromising attack: The second type of possible attack named compromising attack, where the attacker might use its own resources to compromise a fog node to retrieve data stored there. However, the decryption key is stored on the cloud server instead of the fog node, which means the attacker cannot obtain it. Similar to the above eavesdropping attack analysis, even though an attacker obtains the ciphertext stored in the fog node, it cannot recover the original data accurately. Therefore, the proposed scheme can provide strong confidentiality for data stored in the fog node.

2) SECURITY EVALUATION WITH NUMERICAL RESULTS

In this subsection, we will present the security characteristics of our proposed scheme more intuitively through numerical results.

In Fig. 2, we randomly select 40 data generated by one device in a time period (be defined as 5 seconds) as the original data. These data are transmitted over the data link between the sensing layer and the fog layer in the form of ciphertext, and we assume that there is an eavesdropper on the data link. Observing from Fig. 2, we can find that the obtained results of the legal cloud coincide with the original data, which indicates the high recovery accuracy of our developed algorithm. On the contrary, there is a big fluctuation between the obtained data of the eavesdropper and the original data. For example, when the index of the data is 10, the original data is equal to 250, the reconstructed data of the legal cloud is 250, but the obtained data of eavesdropper is 17. The reason for this phenomenon is that the eavesdropper does not have the privacy key, and it is difficult to decrypt the ciphertext. Even if the decryption operation is performed, only inaccurate decryption results can be obtained.

Fig. 3 shows the comparison of obtained results between legal cloud and compromising attacker. The original data denote the stored data in one fog node, which are aggregation results from 14 different IoT devices. As can be seen from the Fig. 3, the decryption results of the legal cloud are perfectly matching with the original data, where the data obtained by the compromising attacker deviate from the original data significantly. For example, when the index of the aggregated data is 5, the original data is equal to 988, the reconstructed data of the legal cloud is 988, nevertheless, the obtained data of attacker is 321. This is because the decryption key is stored on the cloud server, which is not accessible to the fog node and attacker. Hence the compromising attack in fog node does not have the ability to decrypt the encrypted aggregated ciphertext. Even if the attacker performs the decryption operation, they cannot acquire the accurate results. Therefore, it further confirms that the proposed privacy-aware data processing mechanism can effectively resist the compromising attack and the curiosity of fog node.

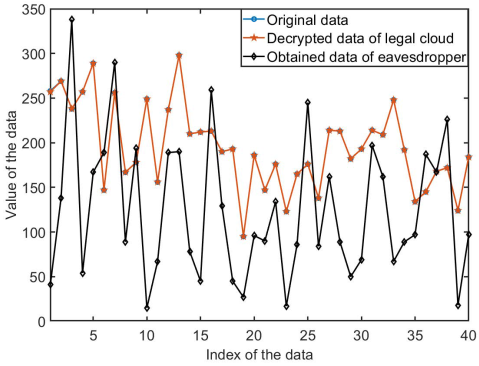

FIGURE 2. The comparison of obtained results between legal cloud and eavesdropper.

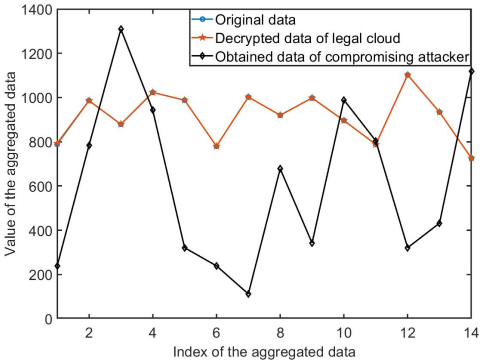

FIGURE 3. The comparison of obtained results between legal cloud and compromising attacker.

B. PERFORMANCE EVALUATION

We assume that the sub-area contains a fog node and 5 IoT sensing devices. The computation capacity and power of each fog node are set as $U_f^{comp} = 30$Mb/s and $P_f^{comp} = 15$W, respectively. Similarly, the computation capacity and power of each sensing device are set as $U_d^{comp} = 10$Mb/s and $P_d^{comp} = 5$W. In the communication environment, we define the bandwidth between the sensing layer and the fog layer to be $B = 25$Mb/s and the white Gaussian noise to be $N_0 = 10^{-10}$W. We set the channel gain as $h = 1$, and set the step size as $s = 0.0001$. The offloading ratios of five devices are respectively set as 0.5, 0.7, 0.8, 0.3 and 0.4; the occupation ratios of fog node's computation capacity assigned to each device are respectively set as 0.1, 0.2, 0.1, 0.1 and 0.2; the initial transmission rates of five devices are respectively set as 5Mb/s, 4Mb/s, 3Mb/s, 4Mb/s and 3Mb/s; and the task sizes of five devices are respectively set as 10Mb, 9Mb, 13Mb, 7Mb and 11Mb.

Fig. 4 compares the energy consumption's convergence rates of the traditional gradient descent and momentum

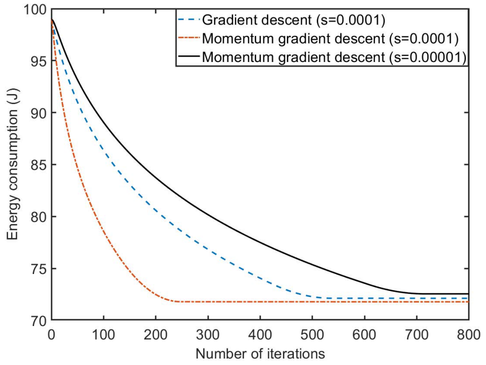

FIGURE 4. Energy consumptions with the traditional gradient descent and momentum gradient descent methods.

gradient descent methods, as well as evaluates the performance of the momentum gradient method in the case of different step sizes. It illustrates that both two different methods can converge to the optimal energy consumption, and the momentum gradient method converges faster than traditional methods under the condition of same step size. This is because each update of the traditional gradient descent method is up to the current gradient value, while the momentum gradient method will update the descent direction according to the previous accumulated momentum and the current gradient. At the same time, it can be seen from this figure that the convergence rate behaves better in the case of larger step size. However, it is not advisable to increase the step size endlessly in order to get a faster convergence speed. If the step size exceeds a certain limit, it will not converge to the optimal value. These simulation results verify the effectiveness of the proposed algorithm and its advantage in convergence speed compared with traditional method.

In the following simulation figures, 'Local computing' represents the method in which all computation tasks are processed in local; 'Full offloading' refers to the method in which all computation tasks are offloaded to the fog node for processing; 'PGCO' indicates the performance guaranteed computation offloading scheme proposed in work [34]; 'Proposed method' represents the scheme proposed in this paper.

Fig. 5 depicts the influence of computation capacity of IoT device on energy consumption. With the increase of IoT device's computation capacity, the energy consumptions of local computing, PGCO and the proposed computation offloading scheme in this paper all present a downward trend, and our proposed scheme has a better performance in energy consumption when compared with other three schemes. Since PGCO scheme does not consider the optimization allocation of occupation ratio of fog node's computation capacity, its energy consumption is higher than our proposed scheme. Meanwhile, we discover that the offloading ratios of all devices show a declining trend. The reason is that as the increase of the IoT devices' computation capacity, the proposed scheme prefers to leave the computation task to be processed in local for decreasing the communication energy consumption. The full offloading scheme remains unchangeableness for its energy consumption is independent of local IoT devices.

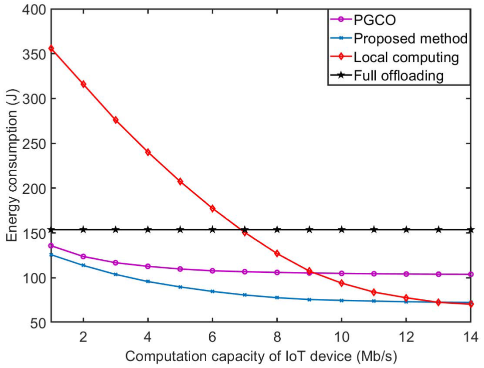

FIGURE 5. The influence of computation capacity of IoT device on energy consumption.

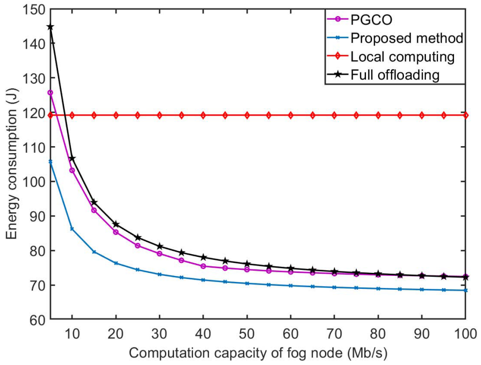

FIGURE 6. The influence of fog node's computation capacity on energy consumption.

Fig. 6 demonstrates the influence of fog node's computation capacity on energy consumption. In Fig. 6, with the increase of the fog node's computation capacity, the energy consumptions of the full offloading scheme, PGCO scheme and our proposed computation offloading scheme all present a downward trend and our proposed scheme is always the best among these four schemes in the term of energy consumption. These simulation results also show that the offloading ratio of each device keeps an increasing trend, which indicates that IoT devices are willing to offload their computation tasks to the corresponding fog node for processing. Because the increase of fog node's computation capacity will obviously enhance the computing efficiency of fog node, and the reduced computation energy consumption can offset the communication energy consumption under the delay constraint. The energy consumption of the local computing scheme does not change under different computation capacities of the fog node for which is independent of fog node's computation capacity.

VI. CONCLUSION

According to the requirements of IoT devices for low energy consumption and high privacy in data processing, this paper develops a privacy and energy co-aware data aggregation computation offloading scheme for fog-assisted IoT networks. The purpose of this proposed scheme is to minimize the total energy consumption of computation tasks with security guarantee, in which a fog-assisted secure three-layer computing architecture and momentum gradient descent based energy-efficient offloading decision algorithm are developed to achieve such goal. Finally, the numerical results validate the superiorities of our proposed scheme in data security, convergence rate and energy consumption. Generally speaking, in a complex and dynamic network, it will have a large number of variables, and which will produce great computing challenge for traditional optimization solutions. In order to overcome this limitation, in our further work, the application of artificial intelligence methods [35], [36], [37] will be considered in the offloading decision process for realizing more efficient computation offloading.

REFERENCES

[1] S. Chen, Z. Wang, H. Zhang, G. Yang, and K. Wang, ‘‘Fog-based optimized kronecker-supported compression design for industrial IoT,’’ *IEEE Trans. Sustain. Comput.*, vol. 5, no. 1, pp. 95–106, Jan. 2020.

[2] A. V. Dastjerdi and R. Buyya, ‘‘Fog computing: Helping the Internet of Things realize its potential,’’ *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[3] T. H. Luan, L. Gao, and Z. Li, ‘‘Fog computing: Focusing on mobile users at the edge,’’ *Comput. Res. Repository*, vol. 24, pp. 11–16, Feb. 2015.

[4] F. Bonomi, R. Milito, and J. Zhu, ‘‘Fog computing and its role in the Internet of Things,’’ in *Proc. Mobile Cloud Comput. Workshop (MCC)*, Aug. 2012, pp. 13–16.

[5] S. Chen, Y. Zheng, W. Lu, V. Varadarajan, and K. Wang, ‘‘Energy-optimal dynamic computation offloading for industrial IoT in fog computing,’’ *IEEE Trans. Green Commun. Netw.*, early access, Dec. 19, 2020, doi: 10.1109/TGCN.2019.2960767.

[6] S. Chen, S. Zhang, X. Zheng, and X. Ruan, ‘‘Layered adaptive compression design for efficient data collection in industrial wireless sensor networks,’’ *J. Netw. Comput. Appl.*, vol. 129, pp. 37–45, Mar. 2019.

[7] C. Zhu, J. Tao, G. Pastor, Y. Xiao, Y. Ji, Q. Zhou, Y. Li, and A. Yla-Jaaski, ‘‘Folo: Latency and quality optimized task allocation in vehicular fog computing,’’ *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4150–4161, Jun. 2019.

[8] W. Tang, J. Ren, K. Zhang, D. Zhang, Y. Zhang, and X. Shen, ‘‘Efficient and privacy-preserving fog-assisted health data sharing scheme,’’ *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–23, Dec. 2019.

[9] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami, ‘‘PPFA: Privacy preserving fog-enabled aggregation in smart grid,’’ *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3733–3744, Aug. 2018.

[10] X. He, Y. Chen, and K. K. Chai, ‘‘Delay-aware energy efficient computation offloading for energy harvesting enabled fog radio access networks,’’ in *Proc. IEEE 87th Veh. Technol. Conf. (VTC Spring)*, Jun. 2018, pp. 1–6.

[11] A. Yousefpour, G. Ishigaki, R. Gour, and J. P. Jue, ‘‘On reducing IoT service delay via fog offloading,’’ *IEEE Internet Things J.*, vol. 5, no. 2, pp. 998–1010, Apr. 2018.

[12] G. Zhang, F. Shen, Y. Yang, H. Qian, and W. Yao, ‘‘Fair task offloading among fog nodes in fog computing networks,’’ in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[13] Q. Wang and S. Chen, ‘‘Latency-minimum offloading decision and resource allocation for fog-enabled IoT networks,’’ *Trans. Emerg. Telecommun. Technol.*, early access, Jan. 28, 2020, doi: 101002/ett.3880.

[14] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, ‘‘Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things,’’ *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.

[15] S. Chen, X. Zhu, H. Zhang, C. Zhao, G. Yang, and K. Wang, ‘‘Efficient privacy preserving data collection and computation offloading for fog-assisted IoT,’’ *IEEE Trans. Sustain. Comput.*, early access, Jan. 22, 2020, doi: 10.1109/TSUSC.2020.2968589.

[16] M. Du, K. Wang, Z. Xia, and Y. Zhang, ‘‘Differential privacy preserving of training model in wireless big data with edge computing,’’ *IEEE Trans. Big Data*, early access, Apr. 24, 2018, doi: 10.1109/TBDATA.2018.2829886.

[17] F. Wang, Y. Xu, L. Zhu, X. Du, and M. Guizani, ‘‘LAMANCO: A lightweight anonymous mutual authentication scheme for N -Times computing offloading in IoT,’’ *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4462–4471, Jun. 2019.

[18] W. Tang, X. Zhao, W. Rafique, and W. Dou, ‘‘A blockchain-based offloading approach in fog computing environment,’’ in *Proc. IEEE Intl Conf Parallel Distrib. Process. Appl., Ubiquitous Comput. Commun., Big Data Cloud Comput., Social Comput. Netw., Sustain. Comput. Commun. (ISPA/IUCC/BDCloud/SocialCom/SustainCom)*, Dec. 2018, pp. 308–315.

[19] M. Min, X. Wan, L. Xiao, Y. Chen, M. Xia, D. Wu, and H. Dai, ‘‘Learning-based privacy-aware offloading for healthcare IoT with energy harvesting,’’ *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4307–4316, Jun. 2019.

[20] Z. Chang, Z. Zhou, T. Ristaniemi, and Z. Niu, ‘‘Energy efficient optimization for computation offloading in fog computing system,’’ in *Proc. IEEE Global Commun. Conf. GLOBECOM*, Dec. 2017, pp. 1–6.

[21] Y.-L. Jiang, Y.-S. Chen, S.-W. Yang, and C.-H. Wu, ‘‘Energy-efficient task offloading for time-sensitive applications in fog computing,’’ *IEEE Syst. J.*, vol. 13, no. 3, pp. 2930–2941, Sep. 2019.

[22] H. Zhu, Z. Zhu, X. Luo, and H. Qian, ‘‘Distributed computation offloading in resource limited fog computing,’’ in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–5.

[23] M. Al-khafajiy, T. Baker, H. Al-Libawy, Z. Maamar, M. Aloqaily, and Y. Jararweh, ‘‘Improving fog computing performance via Fog-2-Fog collaboration,’’ *Future Gener. Comput. Syst.*, vol. 100, pp. 266–280, Nov. 2019.

[24] M. Al-khafajiy, T. Baker, A. Waraich, D. Al-Jumeily, and A. Hussain, ‘‘IoT-fog optimal workload via fog offloading,’’ in *Proc. IEEE/ACM Int. Conf. Utility Cloud Comput. Companion (UCC Companion)*, Dec. 2018, pp. 359–364.

[25] Z. Ali, L. Jiao, T. Baker, G. Abbas, Z. H. Abbas, and S. Khaf, ‘‘A deep learning approach for energy efficient computational offloading in mobile edge computing,’’ *IEEE Access*, vol. 7, pp. 149623–149633, 2019.

[26] Y. Huo, C. Yong, and Y. Lu, ‘‘Re-ADP: Real-time data aggregation with adaptive ω-Event differential privacy for fog computing,’’ *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–13, Jul. 2018.

[27] F. Y. Okay and S. Ozdemir, ‘‘A secure data aggregation protocol for fog computing based smart grids,’’ in *Proc. IEEE 12th Int. Conf. Compat., Power Electron. Power Eng. (CPE-POWERENG)*, Apr. 2018, pp. 1–6.

[28] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, ‘‘APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT,’’ *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[29] X. Xu, B. Tang, G. Jiang, X. Liu, Y. Xue, and Y. Yuan, ‘‘Privacy-aware data offloading for mobile devices in edge computing,’’ in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 170–175.

[30] X. He, R. Jin, and H. Dai, ‘‘Deep PDS-learning for privacy-aware offloading in MEC-enabled IoT,’’ *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4547–4555, Jun. 2019.

[31] X. He, R. Jin, and H. Dai, ‘‘Physical-layer assisted privacy-preserving offloading in mobile-edge computing,’’ in *Proc. ICC IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–6.

[32] X. Liu, X. Xu, Y. Yuan, X. Zhang, and W. Dou, ‘‘Energy-efficient computation offloading with privacy preservation for edge computing-enabled 5G networks,’’ in *Proc. Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2019, pp. 176–181.

[33] P. Paillier, ‘‘Public-key cryptosystems based on composite degree residuosity classes,’’ in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, May 1999, pp. 223–238.

[34] X. Tao, K. Ota, M. Dong, H. Qi, and K. Li, ‘‘Performance guaranteed computation offloading for mobile-edge cloud computing,’’ *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 774–777, Dec. 2017.

[35] X. Zhu, S. Chen, S. Chen, and G. Yang, ‘‘Energy and delay co-aware computation offloading with deep learning in fog computing networks,’’ in *Proc. IEEE 38th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Oct. 2019, pp. 1–6.

[36] Y. Wang, K. Wang, H. Huang, T. Miyazaki, and S. Guo, "Traffic and computation co-offloading with reinforcement learning in fog computing for industrial applications," *IEEE Trans. Ind. Informat.*, vol. 15, no. 2, pp. 976–986, Feb. 2019.

[37] N. Cheng, F. Lyu, W. Quan, C. Zhou, H. He, W. Shi, and X. Shen, "Space/Aerial-assisted computing offloading for IoT applications: A learning-based approach," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 5, pp. 1117–1129, May 2019.

SIGUANG CHEN (Member, IEEE) received the Ph.D. degree in information security from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2011. He finished his Postdoctoral Research work with the City University of Hong Kong, in 2012. From 2014 to 2015, he was a Postdoctoral Fellow with The University of British Columbia. He is currently an Associate Professor with the Nanjing University of Posts and Telecommunications. He has published more than 70 articles and applied 30 patents. His current research interests are in the areas of fog/edge computing, deep/reinforcement learning, privacy preserving of big data, and the IoT resource optimization. He served/serves as a TPC Member in IOP 2015, WCSP 2016, ICCT 2017, 2018, and 2019, CISIS 2018, ICCCS 2018 Workshop, GLOBECOM 2018 Workshop, ICC 2019 and 2020, and ICCC 2019 and 2020. He serves as General Co-Chair of ICAIS/ICCCS 2019 and 2020 Workshop on Mobile, Wireless and Sensors Networking. He also served/serves as the Session Chair of ICCCN 2015, ICCCN 2016, ICCCN 2018, ICC 2018 and 2019, and GLOBECOM 2018. He serves as an Editor for *EAI Endorsed Transactions on Cloud Systems*, the *Journal on Internet of Things*, a Guest Editor for the *International Journal of Computer Networks and Communications*, and a Corresponding Experts of *Engineering Journal*.

ZIHUI YOU received the B.E. degree in the Internet of Things engineering from the Nanjing University of Posts and Telecommunications, in 2018, where she is currently pursuing the master's degree. Her research interests include the Internet of Things, fog computing, and computation offloading.

XIUKAI RUAN was born in Wenzhou, Zhejiang, China, in 1979. He received the B.S. degree in automation engineering from the Zhejiang University of Technology, China, and the M.S. degree in circuits and systems and the Ph.D. degree in signal and information processing from the Nanjing University of Posts and Telecommunications, China. He is currently working as the Dean of the Institute of Intelligent Locks, the Chief Engineer and the Vice Director of the National-local Joint Engineering Laboratory for Digitalized Electrical Design Technology. He has published two monographs. He has authored/coauthored over 70 articles in archival journals. He holds 12 invention patents. His research interests are broadly in the areas of data processing in communication systems, intelligent signal and information processing, and big sensory data. He is also a Commissioner of the Chinese Society of Astronautics and the Chinese Society for Optical Engineering, the Director of the Zhejiang Association of Automation.