sensors

Article

Privacy-Preserving Data Aggregation against False Data Injection Attacks in Fog Computing

Yinghui Zhang [1,2,*], Jiangfan Zhao [1], Dong Zheng [1,2,*], Kaixin Deng [1], Fangyuan Ren [1], Xiaokun Zheng [3] and Jiangang Shu [4]

[1] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China; zjf291495791@163.com (J.Z.); dkx523121943@163.com (K.D.); rfyren@163.com (F.R.)

[2] Westone Cryptologic Research Center, Beijing 100070, China

[3] School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an 710121, China; xiaokzheng@163.com

[4] Department of Computer Science, City University of Hong Kong, Kowloon Tong, Hong Kong, China; jgshu2-c@my.cityu.edu.hk

[*] Correspondence: prrd2007@163.com (Y.Z.); zhengdong@xupt.edu.cn (D.Z.); Tel.: +86-029-88166798 (D.Z.)

Received: 21 June 2018; Accepted: 7 August 2018; Published: 13 August 2018

Abstract: As an extension of cloud computing, fog computing has received more attention in recent years. It can solve problems such as high latency, lack of support for mobility and location awareness in cloud computing. In the Internet of Things (IoT), a series of IoT devices can be connected to the fog nodes that assist a cloud service center to store and process a part of data in advance. Not only can it reduce the pressure of processing data, but also improve the real-time and service quality. However, data processing at fog nodes suffers from many challenging issues, such as false data injection attacks, data modification attacks, and IoT devices' privacy violation. In this paper, based on the Paillier homomorphic encryption scheme, we use blinding factors to design a privacy-preserving data aggregation scheme in fog computing. No matter whether the fog node and the cloud control center are honest or not, the proposed scheme ensures that the injection data is from legal IoT devices and is not modified and leaked. The proposed scheme also has fault tolerance, which means that the collection of data from other devices will not be affected even if certain fog devices fail to work. In addition, security analysis and performance evaluation indicate the proposed scheme is secure and efficient.

Keywords: fog computing; Internet of Things; homomorphic encryption; privacy; data aggregation

1. Introduction

In recent years, cloud computing has developed rapidly with its advantages of ultra-large-scale storage, powerful computing power, high scalability, and low cost [1]. Any company or individual can access cloud computing servers through a payment mode [2–6]. At the same time, with the advancement of computer technology and the development of big data, artificial intelligence, and the Internet of Things (IoT), the demand for data interaction analysis for mass terminals has rapidly increased [7–9]. Under the circumstances, all data files are uploaded to the cloud for processing, which will be given cost and performance pressures to the network. Especially for IoT, it is difficult to meet the low latency requirements of real-time processing [10,11]. In 2012, Cisco proposed the concept of "fog computing" in [12] to address the high latency, the lack of support for mobility and location awareness of cloud computing. The idea is to transfer some of the storage and calculation operations on the cloud to the infrastructure device, that is, fog node, which belongs to the edge network. In other words, fog computing is an extension of cloud computing. The perfect combination of cloud and fog computing makes the network more efficient.

In the smart grid, Internet of Vehicles (IoV), smart home [13], smart health [14] and other IoT application scenarios [15–18], these hybrid IoT devices' data can be sent to the control center through fog nodes. The data often contains user's privacy [19–24]. For instance, heart monitors are related to the life safety of each user [25], and smart meters in smart grid collect power data which reflects users' daily lives [26–29]. In smart grid, a power company collects smart meter's data and analyzes them to ensure that the power system runs efficiently [30].

Because the fog nodes are deployed at the edge of the network and low-traffic nodes, they are more vulnerable to hackers. Once user's information is leaked, it will have a bad influence [31], and the sensitive data must be encrypted before uploading [32,33]. In addition, when a large number of IoT device data is transmitted to fog nodes, it will not only affect the requirements for a real-time response of IoT, but also cause problems such as network congestion. At this time, the data aggregation based on homomorphic encryption applied to fog devices is particularly important [34–37]. Specifically, when the fog device sends the aggregated data instead of the data of each IoT device to the control center, the communication overhead will be greatly reduced, although the security and privacy issues are needed to be addressed [38]. In fact, data aggregation technology is widely used in various communication networks to save bandwidth [39–44].

In this paper, we propose a privacy-preserving data aggregation scheme based on homomorphic encryption in fog computing (PDAF). At a time slot, each IoT device will report its sensing data to a fog node after the data is blinded by two secret keys and a blinding factor. The data is then collected by the control center so that the entire IoT network runs efficiently. These blinded data are aggregated by fog devices at the edge of the network. All the aggregated values are sent by the fog device to the control center, and the fog device is able to detect faulty IoT devices. Upon receiving the packet, the control center can generate relevant secret keys and get the total amount of IoT devices' sensing data at each time slot from the aggregated blinded data. For the sake of security, packets transmitted during the communication process should be verified. In the PDAF system, only the control center can know the total amount of IoT devices' sensing data at each time slot, and individual IoT device data is hidden. Our security and privacy analysis indicates that PDAF is secure against false data injection attacks and data modification and it can protect data privacy. Extensive evaluations show that PDAF is very efficient in terms of the computation and communication cost.

1.1. Related Work

In 2004, the International Telecommunication Union (ITU) expanded the concept of the IoT: Interconnections at any time, anywhere, arbitrary objects, ubiquitous networks and ubiquitous computing [45]. Cisco [12] pointed that the Internet of Things as a delay-sensitive application, which requires high real-time performance. In the era of the Internet of Everything, a new platform called fog computing is needed to support it. The author considered fog computing as a new application and service, and that there is a fruitful interaction between cloud and fog, especially in data management and analysis. In simple terms, the fog is a cloud close to the ground.

In IoT, in order to reduce communication costs, it is essential to aggregate individual IoT device's data at associated fog device. In the previous researches, some privacy-preserving data aggregation schemes [10,26,27,30,37,46] are related to our PDAF scheme. In addition, blockchain technologies have been used for realizing fair payment in cloud computing and fog computing [47–49]. Zhang et al. [27] designed a privacy-preserving communication and power injection scheme over vehicle networks and 5G smart grid slice based on the Paillier encryption. In the scheme, a novel aggregation technique called hash-then-homomorphic is used to aggregate the blinded bids of different time slots. Mahmoud et al. [30] adopted two data different aggregation schemes using point addition and homomorphic encryption. Shen et al. [37] proposed a privacy-preserving multilevel user's data aggregation and control scheme, it extended the previous one-dimensional data aggregation to two dimensions and is more suitable for practical application environments. Zhou et al. [46] also proposed a multidimensinal data aggregation scheme and is fault-tolerant. However, Zhang et al. [26] considered the EPPI scheme based on point addition is safer and more efficient. In fact, EPPI guarantees that privacy will not be leaked even if all entities in the actual application scene are dishonest. But the EPPI scheme is not fault-tolerant. Although the above schemes are suitable for fog computing-enhanced IoT, they cannot aggregate all hybrid IoT devices' data into a single ciphertext. For fog computing-enhanced IoT, Lu et al. [10] designed a lightweight privacy-preserving data aggregation scheme which is secure and fault-tolerant, but the third-party trusted authority in this system will inevitably increase the communication overhead of the system. Different from the above schemes, in PDAF, the third-party trusted authority is not needed and data privacy is still preserved. We use the modified Paillier encryption to enable the fog device to aggregate hybrid IoT devices' data into a single ciphertext and keep it fault-tolerant.

1.2. Our Contribution

In PDAF, we have made improvements based on the Paillier homomorphic encryption scheme, each IoT device can generate two secret key and a blinding factor to mask its sensitive data, and it sends the masked data to the related fog node based on wireless network. Upon receiving packets from all hybrid IoT devices, the control center can only obtain the total within the limited range instead of directly reading data of a single IoT device. Because of the blinding factor, the control center also can correctly decrypt the aggregated data in the event that an IoT device fails to send messages to the fog device. In fact, the proposed PDAF scheme is fault-tolerant. In the second place, the PDAF scheme realizes privacy protection. We notice that the fog device and the control center are curious about the sensitive data to be reported by a single IoT device or the aggregated data by the fog device. In PDAF, the attacker will not get any privacy about the user, nor can it forge or change the ciphertext to be sent to the fog device. In addition, an efficient batch verification method is adopted in order to verify the signatures of multiple users instead of verifying one by one and the computation overhead of the fog device is reduced.

1.3. Organization

The remaining of this paper is organized as follows. In Section 2, we introduce our system model and review some preliminary knowledge. Then, we describe the proposed PDAF scheme in detail in Section 3. Next, we give the security and privacy analysis of the proposed PDAF scheme in Section 4, followed by performance evaluation in Section 5. Finally, in Section 6, we draw our conclusions.

2. Models and Security Requirements

In this section, we formalize our system model, adversary model, security requirements and design goal, and give a brief review on preliminary knowledge which will serve as the building blocks of the proposed PDAF scheme.

2.1. System Model

As shown in Figure 1, the considered system model of PDAF includes a control center, some fog devices at the network edge, and some hybrid IoT devices, which each hybrid IOT device involves a set of heterogeneous IoT devices $U = \{HID_1, HID_2, ..., HID_n\}$.

- Control center. During communication, the control center generates system parameters and is responsible for registration of fog devices and IoT devices. It also collects all IoT devices data $(m_1, m_2, ..., m_n)$ via fog devices periodically and analyzes the data replied by fog devices. Please note that CC cannot directly get $m_i (1 \leq i \leq n)$ which containing the user's privacy. In addition, when an IoT device fails to send a message, it is also necessary to make the aggregation of other users' information unaffected. where, the control center communicates with the IoT devices via the Internet network.

- Fog devices. A fog device is also a fog node and is the most critical part of the fog computing between the hybrid IoT devices and the control center. Fog devices can be memory routers, small servers or smart phones that are deployed at the edge network. In PDAF, the fog device will forward data packets from the control center to IoT devices in their jurisdictions, aggregate all IoT devices' data, and discover faulty IoT devices and report to control center for countermeasures.
- Hybrid IoT devices. With sensing and communication capabilities, the IoT devices HID_i $(i = 1, 2, ..., n)$ are deployed at an area in need and enable to periodically report its sensing result m_i to control center through the relevant fog device.

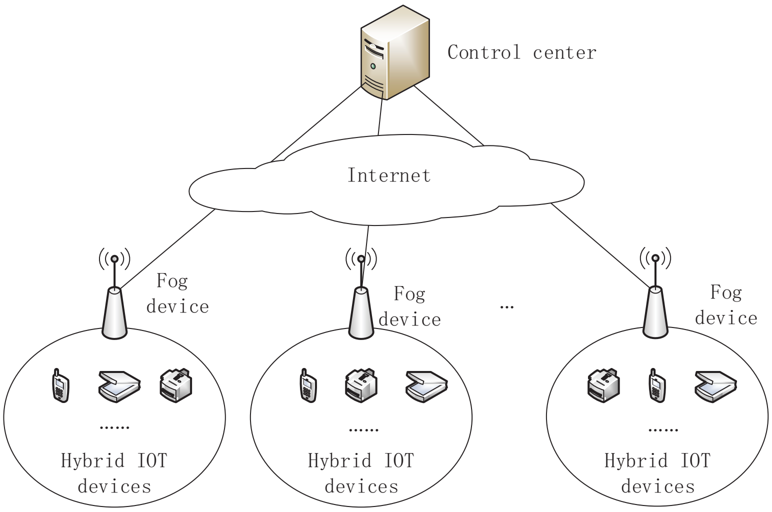

Figure 1. The system model of PDAF.

2.2. Adversary Model

In the proposed PDAF scheme, we assume all the entities are "honest-but-curious". More specifically, they can legitimately do their assigned tasks, but are also curious about the privacy of IoT devices, such as the control center that can intercept data from a single IoT device to gain private information about the device owner and other financial benefits information. Please note that although the entities are "curious", they cannot collude. Similarly, each IoT device also wants to know the data of other IoT devices to determine if it is profitable. In addition, certain IoT devices may fail and stop to report for some time. Here, we assume that each IoT device can only send packets within this fog computing coverage area. It is also possible that an attacker resides between an IoT device and the control center and tries to establish two scert keys such that the IoT device and the control center seems to communication directly. In addition, some IoT attackers and outsiders are also interested in other sensitive information in the fog computing. In PDAF, we focus on the privacy-preserving data aggregation, in which false data injection attacks and data modification can be prevented.

2.3. Security Requirements and Design Goal

Considering the IoT and fog computing practical application environment, in order to prevent from these attackers getting sensitive data of IoT devices, our scheme should meet the following security requirements:

(1) Privacy Protection. Even if the attacker intercepts the communication data transmitted on the insecure channel, it cannot obtain the sensitive data of the IoT devices. The control center can decrypt the aggregated data but cannot get the individual information of a single device.

(2) Non-Repudiation and Unforgeability. The control center and the fog devices can verify the received data packets to ensure that the data packets come from the legal unit and has not been tampered, that is, the proposed scheme can defeat the false injection attack and detect the malicious attack. Besides, the adversary should not impersonate the control center, the fog devices, or the IoT devices.

Under the considered system model and security requirements, our design goal is to propose a privacy-preserving data aggregation scheme based on homomorphic encryption in fog computing. First, private data of IoT devices cannot be compromised. Second, the proposed scheme should be fault-tolerant. When certain IoT devices fail to work, they should be detected by the associated fog device and reported to the control center. Third, the control center and the fog device are able to authenticate the received packets to make sure that the packets have not been modified during the transmission and are really from legal IoT devices. Finally, if the proposed scheme effectively reduces the amount of channel transmission and improves the data processing efficiency of each entity, then the proposed scheme will be more practical.

3. Proposed PDAF Scheme

In this section, we propose a privacy-preserving data aggregation scheme based on homomorphic encryption in fog computing, which consists of the following parts: preliminaries, system initialization, data collection request, hybrid IoT devices report, privacy-preserving aggregated data generation, privacy-preserving aggregated data decryption, and fault tolerance mechanism. Figure 2 summarizes the six phases of the proposed scheme. The details are given in the following:

3.1. Preliminaries

In this subsection, we give a brief review of bilinear pairings and the Paillier encryption algorithm.

3.1.1. Bilinear Pairings

Let G_1, G_2 be a cyclic addition group and a cyclic multiplication group of prime order q and $P_0 \in G_1$ be a generator. We call $\hat{e}$ a bilinear pairing if $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ is a map with the following properties:

(1) Bilinear: For all $a, b \in Z_q^*$, $\hat{e}(aP_0, bP_0) = \hat{e}(P_0, P_0)^{ab}$.
(2) Non-degenerate: $\hat{e}(P_0, P_0) \neq 1_{G_1}$.
(3) Computable: For all $P_0, Q \in G_1$, there is an efficient algorithm to compute $\hat{e}(P_0, Q)$.

3.1.2. Paillier Encryption Algorithm

Paillier encryption is a homomorphic encryption algorithm that consists of three algorithms: key generation, encryption, and decryption. The special as follow:

- Key Generation: Given a safety parameter κ, choose two large primes p and q, where $\mid p \mid = \mid q \mid = \kappa$, compute $N = pq$ and $\lambda = lcm(p-1, q-1)$, define the function $L(u) = \frac{u-1}{N}$, select the generator $g \in Z_{N^2}^*$ and get the public key $pk = (N, g)$ and the secret key λ.
- Encryption: Given a message $M \in Z_N$, a random number $r \in Z_N^*$ and calculate the ciphertext $C = g^M \cdot r^N \ mod \ N^2$.
- Decryption: Given ciphertext $C \in Z_{N^2}^*$, the corresponding plaintext is $M = \frac{L(C^\lambda mod N^2)}{L(g^\lambda mod N^2)} \ mod \ N$.

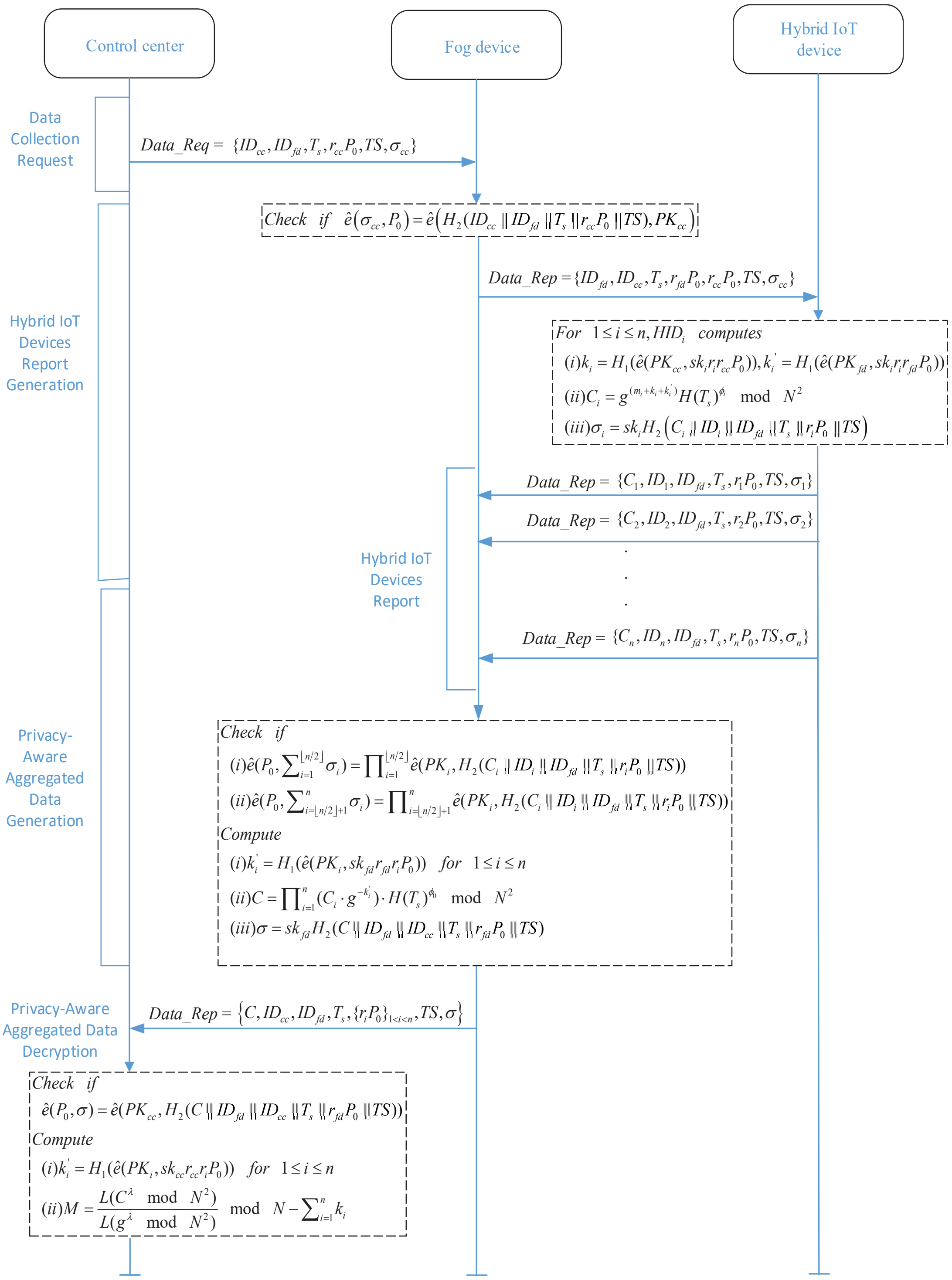
Control center
Fog device
Hybrid IoT device
Data Collection Request
$Data\_Req = \{ID_{cc}, ID_{fd}, T_s, r_{cc}P_0, TS, \sigma_{cc}\}$
$Check\ \ if\ \ \hat{e}(\sigma_{cc}, P_0) = \hat{e}(H_2(ID_{cc} \| ID_{fd} \| T_s \| r_{cc}P_0 \| TS), PK_{cc})$
Hybrid IoT Devices Report Generation
$Data\_Rep = \{ID_{fd}, ID_{cc}, T_s, r_{fd}P_0, r_{cc}P_0, TS, \sigma_{cc}\}$
$For\ \ 1 \le i \le n, HID_i\ \ computes$
$(i) k_i = H_1(\hat{e}(PK_{cc}, sk_i r_i r_{cc} P_0)), k_i^{'} = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{fd} P_0))$
$(ii) C_i = g^{(m_i + k_i + k_i^{'})} H(T_s)^{\phi_i} \mod N^2$
$(iii) \sigma_i = sk_i H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS)$
Hybrid IoT Devices Report
$Data\_Rep = \{C_1, ID_1, ID_{fd}, T_s, r_1P_0, TS, \sigma_1\}$
$Data\_Rep = \{C_2, ID_2, ID_{fd}, T_s, r_2P_0, TS, \sigma_2\}$
$Data\_Rep = \{C_n, ID_n, ID_{fd}, T_s, r_nP_0, TS, \sigma_n\}$
Privacy-Aware Aggregated Data Generation
$Check\ \ if$
$(i) \hat{e}(P_0, \sum_{i=1}^{\lfloor n/2 \rfloor} \sigma_i) = \prod_{i=1}^{\lfloor n/2 \rfloor} \hat{e}(PK_i, H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS))$
$(ii) \hat{e}(P_0, \sum_{i=\lfloor n/2 \rfloor + 1}^{n} \sigma_i) = \prod_{i=\lfloor n/2 \rfloor + 1}^{n} \hat{e}(PK_i, H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS))$
$Compute$
$(i) k_i^{'} = H_1(\hat{e}(PK_i, sk_{fd} r_{fd} r_i P_0))\ \ for\ \ 1 \le i \le n$
$(ii) C = \prod_{i=1}^{n} (C_i \cdot g^{-k_i^{'}}) \cdot H(T_s)^{\phi_0} \mod N^2$
$(iii) \sigma = sk_{fd} H_2(C \| ID_{fd} \| ID_{cc} \| T_s \| r_{fd} P_0 \| TS)$
Privacy-Aware Aggregated Data Decryption
$Data\_Rep = \{C, ID_{cc}, ID_{fd}, T_s, \{r_iP_0\}_{1<i<n}, TS, \sigma\}$
$Check\ \ if$
$\hat{e}(P_0, \sigma) = \hat{e}(PK_{cc}, H_2(C \| ID_{fd} \| ID_{cc} \| T_s \| r_{fd} P_0 \| TS))$
$Compute$
$(i) k_i^{'} = H_1(\hat{e}(PK_i, sk_{cc} r_{cc} r_i P_0))\ \ for\ \ 1 \le i \le n$
$(ii) M = \frac{L(C^{\lambda} \mod N^2)}{L(g^{\lambda} \mod N^2)} \mod N - \sum_{i=1}^{n} k_i$

Figure 2. Six phases of PDAF.

3.2. Details of PDAF

3.2.1. System Initialization

(1) System parameters generated: In the system parameters generation stage, the control center (CC) selects the security parameter κ and generates $(q, P_0, G_1, G_2, \hat{e})$ by running $gen(\kappa)$. Then, CC selects g as a generator of $Z_{N^2}^*$, the security parameter κ_1 and two safe large prime

numbers p, q. Computing a homomorphic encryption public key pair $(N = p_1 q_1, g)$ and the corresponding private key $\lambda = lcm(p_1 - 1, q_1 - 1)$. Next, CC defines a function $L(x) = \frac{x-1}{N}$ and chooses five secure cryptographic hash functions, $H : \{0,1\}^* \rightarrow Z_N^*$, $H_1 : G_2 \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow G_1$, $H_3 : \{0,1\}^* \rightarrow Z_q^*$, $H_4 : G_1 \rightarrow Z_q^*$ and a random element sk_{cc} as its secret key and calculates $PK_{cc} = sk_{cc}P_0$ as its public key. Finally, CC publishes the public parameters $\{(q, P_0, G_1, G_2, \hat{e}, N, H, H_1, H_2, H_3, H_4\}$.

(2) Registration:

- Fog Devices Registration.
  The fog device (FD) chooses a random element sk_{fd} as its secret key and calculates $PK_{fd} = sk_{fd}P_0$ as its public key. Choosing random number $x \in Z_q^*$ and calculating $\alpha = H_3(x \parallel ID_{fd})P_0$, $\beta = H_3(x \parallel ID_{fd}) - sk_{fd}H_4(\alpha)$ *mod q*, where, ID_{fd} is the identity of the fog device. Then, FD sends the parameters $\{PK_{fd}, \alpha, \beta, ID_{fd}\}$ to CC. After receiving the parameters $\{PK_{fd}, \alpha, \beta, ID_{fd}\}$, CC verifies whether the equation $\alpha = \beta P_0 + H_4(\alpha)PK_{fd}$ holds. If passed, CC publishes the public parameters $\{PK_{fd}, ID_{fd}\}$, otherwise, refused to register.
- Hybrid IoT Devices Registration. HID$_i(i = 1, 2, ..., n)$ chooses a random element sk_i as its secret key and calculates $PK_i = sk_iP_0$ as its public key. HID$_i$ Chooses random number $x_i \in Z_q^*$ and calculates $\alpha_i = H_3(x_i \parallel ID_i)P_0$, $\beta_i = H_3(x_i \parallel ID_i) - sk_iH_4(\alpha_i)$ *mod q*, where, ID_i is the identity of the hybrid IoT device. Then, HID$_i$ sends the parameters $\{PK_i, \alpha_i, \beta, ID_i\}$ to CC. After receiving the parameters $\{PK_i, \alpha_i, \beta, ID_i\}$, CC verifies whether the equation $\alpha_i = \beta_iP_0 + H_4(\alpha_i)PK_i$ holds. If passed, CC publishes the public parameters $\{PK_i, ID_i\}$, otherwise, refused to register.

(3) Blinding Factor Generated: After completing the registration, CC runs pseudo-random generator and generates n random numbers $\phi_i \in Z_N$ as a blinding factor for HID$_i$ under each FD region and computers $\phi_0 = -(\phi_1 + \phi_2 + ... + \phi_n \ mod\ N)$ as FD's blinding factor. Please note that ϕ_i and ϕ_0 are satisfied $\sum_{i=0}^{n} \phi_i \equiv 0 \ mod\ N$. Then, CC sends ϕ_0 to the registered FD, and sends ϕ_i to the registered HID$_i$.

3.2.2. Data Collection Request

In PDAF, the control center can collect data from related fog devices during every time slot T_s. To be specific, CC sends data collection request (*Data_Req*) packet that contains parameters $\{ID_{cc}, ID_{fd}, T_s, r_{cc}P_0, TS, \sigma_{cc}\}$ to fog devices. Where, ID_{cc} and ID_{fd} is the identity of the control center and fog device respectively. Please note that $r_{cc} \in Z_q^*$ is a random number, each IOT device uses the secret key $r_{cc}P_0$ to establish a one-time key shared with the control center. Timestamp TS and $\sigma_{cc} = sk_{cc}H_2(ID_{cc} \| ID_{fd} \| T_s \| r_{cc}P_0 \| TS)$ will be used for verifying by the fog devices. Then, the fog device runs the following steps after receiving the *Data_Req* packet:

(1) According to the difference between the current time and the timestamp TS, FD checks the freshness of *Data_Req* packet.

(2) FD verifies the signature by computing if $\hat{e}\ (\sigma_{cc}, P_0) = \hat{e}\ (H_2(ID_{cc} \| ID_{fd} \| T_s \| r_{cc}P_0 \| TS), PK_{cc})$ holds.

(3) If the above equation holds, FD randomly chooses $r_{fd} \in Z_q^*$, calculates $r_{fd}P_0$, puts $r_{fd}P_0$ in the packet *Data_Req*, and broadcasts the packet that contains parameters $\{ID_{fd}, ID_{CC}, T_s, r_{fd}P_0, r_{cc}P_0, TS, \sigma_{cc}\}$ in its area. Please note that $r_{fd}P_0$ is used by hybrid IOT device HID$_i$ covered by the fog device in establishing a one-time key shared with the fog device.

3.2.3. Hybrid IoT Devices Report Generation

After receiving the packet *Data_Req*, hybrid IoT device HID$_i$ will report its sensing data m_i to fog device at time slot T_s. Specific steps are as follows:

(1) The hybrid IoT device HID$_i$ chooses $r_i \in z_q^*$, computers r_iP_0 which is used by ID$_{fd}$ in establishing a shared one-time key between itself and the related fog device.

(2) HID$_i$ computes two shared keys as $k_i = H_1(\hat{e}(PK_{cc}, sk_i r_i r_{cc} P_0))$, $k_i^{'} = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{fd} P_0))$, which will be used for hiding HID$_i$'s sensing data m_i.

(3) HID$_i$ masks its sensing data m_i and computes ciphertext C_i and signature σ_i, where

$$C_i = g^{m_i + k_i + k_i^{'}} H(T_s)^{\phi_i} \ mod \ N^2,$$

$$\sigma_i = sk_i H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS).$$

Then HID$_i$ sends data collection reply *Data_Rep* packet that contains parameters $\{C_i, ID_i, ID_{fd}, T_s, r_i P_0, TS, \sigma_i\}$ to fog devices.

3.2.4. Privacy-Preserving Aggregated Data Generation

Upon receiving the *Data_Rep* packet, the fog device runs the following steps:

(1) FD verifies n *Data_Rep* packets received to ensure that the packets are valid and have not been tampered or forged during communication. To improve the verification efficiency, FD randomly divides the *Data_Rep* packet set $S = (ID_i, ID_{fd}, T_s, r_i P_0, TS, \sigma_i)$ $(i = 1, 2, ..., n)$. From S, $\lfloor n/2 \rfloor$ *Data_Rep* packets are randomly selected to form the first subset S_1, and the remaining $\lceil n/2 \rceil$ *Data_Rep* packets constitute the second subset S_2. For ease of description, suppose S_1 contains the first $\lfloor n/2 \rfloor$ *Data_Rep* packets and S_2 contains the second $\lceil n/2 \rceil$ *Data_Rep* packets. For IOT devices, the *Data_Rep* packets in S_1 are valid if the following equation holds, otherwise the packets are invalid.

$$\hat{e}(P_0, \sum_{i=1}^{\lfloor n/2 \rfloor} \sigma_i) = \prod_{i=1}^{\lfloor n/2 \rfloor} \hat{e}(PK_i, H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS).$$

Note that using the above verification method, the number of bilinear pairs can be reduced from $2\lfloor n/2 \rfloor$ to $\lfloor n/2 \rfloor + 1$. Similarly, FD verifies the following equation. If it holds, the number of bilinear pairs also drops from $2\lfloor n/2 \rfloor$ to $\lfloor n/2 \rfloor + 1$.

$$\hat{e}(P_0, \sum_{i=\lfloor n/2 \rfloor + 1}^{n} \sigma_i) = \prod_{i=\lfloor n/2 \rfloor + 1}^{n} \hat{e}(PK_i, H_2(C_i \| ID_i \| ID_{fd} \| T_s \| r_i P_0 \| TS).$$

(2) If the step 1 is verified, the fog device calculates

$$k_i^{'} = H_1(\hat{e}(PK_i, sk_{fd} r_{fd} r_i P_0)) = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{fd} P_0)).$$

Then, It runs the following data aggregation operations and get the aggregate ciphertext C and the corresponding signature σ, the specific process are as follows:

$$\begin{aligned} C &= \prod_{i=1}^{n} (C_i \cdot g^{-k_i^{'}}) \cdot H(T_s)^{\phi_0} \ mod \ N^2 \\ &= \prod_{i=1}^{n} (g^{m_i + k_i + k_i^{'}} \cdot g^{-k_i^{'}}) \cdot H(T_s)^{\phi_0} \ mod \ N^2 \\ &= g^{\sum_{i=1}^{n} (m_i + k_i)} \cdot H(T_s)^{\sum_{i=0}^{n} \phi_i} \ mod \ N^2 \\ &= g^{\sum_{i=1}^{n} (m_i + k_i)} \cdot H(T_s)^{\beta N} \ mod \ N^2, \\ \sigma &= sk_{fd} H_2(C \| ID_{fd} \| ID_{cc} \| T_s \| r_{fd} P_0 \| TS). \end{aligned}$$

where, because $\sum_{i=0}^{n} \phi_i = 0 \ mod \ N$, $\sum_{i=0}^{n} \phi_i = \beta N$.

(3) The fog device sends the *Data_Rep* packet that contains parameters $\{C, ID_{cc}, ID_{fd}, T_s, \{r_i P_0\}_{1<i<n}, TS, \sigma\}$ to control center.

3.2.5. Privacy-Preserving Aggregated Data Decryption

Upon receiving the fog device reply packet *Data_Rep*, CC first verifies the *Data_Rep* to ensure the packets' authenticity and integrity according to the following equation:

$$\hat{e}(P_0, \sigma) = \hat{e}(PK_{cc}, H_2(C \| ID_{fd} \| ID_{cc} \| T_s \| r_{fd}P_0 \| TS).$$

If it does hold, then CC calculates

$$k_i = H_1(\hat{e}(PK_i, sk_{cc} r_{cc} r_i P_0)) = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{cc} P_0)).$$

Finally, it uses the private key λ to decrypt the aggregated ciphertext C by calculating

$$\begin{aligned} M &= \frac{L(C^{\lambda}\ mod\ N^2)}{L(g^{\lambda}\ mod\ N^2)}\ mod\ N - \sum_{i=1}^{n} k_i \\ &= \sum_{i=1}^{n} m_i. \end{aligned}$$

3.2.6. Fault Tolerance Mechanism

If some hybrid IoT devices breakdown, FD will not receive n *Data_Rep* packets. Then this phenomenon will directly affect the main features of the blinding factor, and $\sum_{i \in U_i / U_i^{'}} \phi_i + \phi_0 \neq 0\ mod\ N$, which will affect the correctness of the final data decryption. Where, U_i means the set of all legitimate hybrid IoT devices and $\mathrm{U}_i^{'}$ means the set of failed hybrid IoT devices ($\mathrm{U}_i^{'} \in \mathrm{U}_i$).

FD needs to send the set $\mathrm{U}_i^{'}$ to control center. After receiving the set $\mathrm{U}_i^{'}$, CC computes $H^{'}(T_s) = H(T_s)^{\sum_{i \in U_i^{'}} \phi_i}$ and replies to FD. After receiving $H^{'}(T_s)$, computing

$$\begin{aligned} C^{'} &= H^{'}(T_s) \cdot \prod_{i \in U_i / U_i^{'}} (C_i \cdot g^{-k_i^{'}} \cdot H(T_s)^{\phi_0})\ mod\ N^2 \\ &= H(T_s)^{\sum_{i \in U_i^{'}} \phi_i} \cdot \prod_{i \in U_i / U_i^{'}} (g^{m_i + k_i + k_i^{'}} \cdot g^{-k_i^{'}} \cdot H(T_s)^{\phi_0})\ mod\ N^2 \\ &= \prod_{i \in U_i / U_i^{'}} g^{(m_i + k_i)} \cdot H(T_s)^{\sum_{i \in U_i^{'}} \phi_i + \sum_{i \in U_i / U_i^{'}} \phi_i + \phi_0}\ mod\ N^2 \\ &= g^{\sum_{i \in U_i / U_i^{'}} (m_i + k_i)} \cdot H(T_s)^{\sum_{i=0}^{n} \phi_i}\ mod\ N^2 \\ &= g^{\sum_{i \in U_i / U_i^{'}} (m_i + k_i)} \cdot H(T_s)^{\beta N}\ mod\ N^2. \end{aligned}$$

At this time, in aggregated data decryption stage, CC uses the private key λ to decrypt the aggregated ciphertext C by calculating.

$$\begin{aligned} M^{'} &= \frac{L(C^{'\lambda}\ mod\ N^2)}{L(g^{\lambda}\ mod\ N^2)}\ mod\ N - \sum_{i \in U_i / U_i^{'}} k_i \\ &= \sum_{i \in U_i / U_i^{'}} m_i. \end{aligned}$$

4. Security and Privacy Analysis

In this section, we give the security and privacy analysis of the proposed PDAF scheme.

4.1. Privacy Protection

Based on the Paillier encryption algorithm, in the hybrid IoT devices report generation stage, the sensitive data m_i was blinded and the secret key k_i and $k_i^{'}$ were added in the Paillier encryption algorithm to get the ciphertext $C_i = g^{m_i+k_i+k_i^{'}} H(T_s)^{\phi_i}\ mod\ N^2$, HID$_i$ sends C_i to the associated gateway instead of m_i directly. Without the private key, it is infeasible to decrypt ciphertexts. Even if the adversary gets the data packet sent by tapping the wireless IoT device or the wireless communication channel, without knowing k_i, $k_i^{'}$ and λ, the adversary cannot know the sensitive data m_i because of these secret keys cannot be computed. Despite the control center has the secret key k_i and λ, it cannot get $k_i^{'}$, and thus cannot decrypt C_i to recover m_i. Similarly, the fog device is also unable to read sensitive data m_i without k_i and λ. In fact, $k_i = H_1(\hat{e}(PK_{cc}, sk_i r_i r_{cc} P_0))$ and $k_i^{'} = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{fd} P_0))$ are computed by HID$_i$. It is worth noting that the fog device only calculates $k_i^{'} = H_1(\hat{e}(PK_i, sk_{fd} r_{fd} r_i P_0)) = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{fd} P_0))$ at the privacy-preserving aggregated data generation phase and the control center only calculates $k_i = H_1(\hat{e}(PK_i, sk_{cc} r_{cc} r_i P_0)) = H_1(\hat{e}(PK_{fd}, sk_i r_i r_{cc} P_0))$ at the privacy-preserving aggregated data decryption phase.

In the data aggregation stage, the aggregation operation by the fog device is performed in a ciphertext manner. For the control center, it only has the aggregated data $M = \frac{L(C^{\lambda}\ mod\ N^2)}{L(g^{\lambda}\ mod\ N^2)}\ mod\ N - \sum_{i=1}^{n} k_i$ and just gets the data sum $\sum_{i=1}^{n} m_i$. Even if an adversary has intruded into the control center database, privacy of a single device cannot be obtained. Like this, the individual sensing data privacy is still preserved.

4.2. Non-Repudiation and Unforgeability

In the proposed PDAF scheme, the private key is also used to sign the data packet to be sent by each entity before sending the message. Then, the data packet is verified based on the sender's public key. Although the process can be realized by homomorphic signatures and the verification method used in database [50–53], the efficiency is very low. In PDAF, it is ensured that adversaries cannot forge a new signature by eavesdropping on signed messages and thus cannot implement forgery attacks. In other words, the entities' private keys are properly kept by themselves, their messages sent has non-repudiation. Our program has the ability to discover the dishonest behavior of entities.

If the traditional one-to-one verification method is used, assuming that there are k signatures to be verified, a total of $2k$ bilinear pairing operations are required. To improve verification efficiency, we use a batch verification method. As described in step 1 of Section 3.2.4, k signatures are randomly assigned to equal-sized sets S_1 and S_2, where $|S_1| = \lfloor \frac{k}{2} \rfloor$, $|S_2| = \lceil \frac{k}{2} \rceil$. Then the signatures in S_1 and S_2 are respectively verified, that is

$$\hat{e}(P_0, \sum_{j \in S_1} \sigma_j) = \prod_{j \in S_1} \hat{e}(PK_j, H_2(C_j \| ID_{INFORMATION} \| TS),$$

$$\hat{e}(P_0, \sum_{j \in S_2} \sigma_j) = \prod_{j \in S_2} \hat{e}(PK_j, H_2(C_j \| ID_{INFORMATION} \| TS).$$

Based on the above batch verification method, the number of bilinear pairing operations is reduced from $2k$ to $2(\lfloor \frac{k}{2} \rfloor + 1)$, and hence the efficiency of the algorithm is improved. Note that, the verification method can resist forgeries. For example, if the adversary aims to generate a forgery by computing

$$\sigma_i^{'} = \begin{cases} \sigma_i - a,\ i = 1, 2, ..., \lfloor \frac{k}{2} \rfloor \\ \sigma_i + a,\ i = \lfloor \frac{k}{2} \rfloor + 1, \lfloor \frac{k}{2} \rfloor + 2, ..., k. \end{cases}$$

In this case, the greatest probability that the adversary forges a valid signature is

$$C_{k/4}^{k/2} C_{k/4}^{k/2} = \frac{(k/2)!}{(k/4)!(k/2 - k/4)!} \cdot \frac{(k/2)!}{(k/4)!(k/2 - k/4)!} \cdot \frac{(k/2)!(k/2)}{k!}.$$

Obviously, when k is large enough, the above probability is negligible.

5. Performance Evaluation

In this section, the performance of the proposed PDAF scheme is evaluated in terms of the computation costs and communication overhead at the IoT devices, the fog device, and the control center.

5.1. Computation Cost

The proposed PDAF scheme achieves the privacy-preserving aggregation for hybrid IoT devices, in order to analyze this scheme more accurately, in terms of computation costs, we assume that there are n IoT devices associated with a fog device and will focus on measuring the time required for performing the cryptographic operations in the proposed scheme. where, we denote the computation costs of an exponentiation operation in G_1, an exponentiation operation in G_2, an exponentiation operation in $Z_{N^2}^*$, a multiplication operation in $Z_{N^2}^*$, a bilinear pairing operation and a Paillier decryption operation with T_{e_1}, T_{e_2}, T_{e_Z}, T_{m_Z}, T_p, T_{pai}, respectively.

For the control center, in order to generate a data collection request, CC needs to calculate $r_{cc}P_0$ and $\sigma_{cc} = sk_{cc}H_2(ID_{cc}\|ID_{fd}\|T_s\|r_{cc}P_0\|TS)$ which need $2T_{e_1}$ computation costs. In privacy-preserving aggregated data decryption phase, CC checks if $\hat{e}(P_0, \sigma) = \hat{e}(PK_{cc}, H_2(C\|ID_{fd}\|ID_{cc}\|T_s\|r_{fd}P_0\|TS)$, computers $k_i^{'} = H_1(\hat{e}(PK_i, sk_{cc}r_{cc}r_iP_0))$ and recovers the aggregated data M respectively involves $2T_p$, $T_p + T_{e_2}$ and T_{pai} computation costs. Therefore, in time slot T_s, the computation cost for the control center is $3T_p + 2T_{e_1} + T_{e_2} + T_{pai}$. For the fog device, it needs $(n+5)T_p + (n+1)T_{m_Z} + 2T_{e_1} + 2T_{e_Z} + T_{e_2}$ computation costs. Specifically, FD checks if $\hat{e}\ (\sigma_{cc}, P_0) = \hat{e}\ (H_2(ID_{cc}\|ID_{fd}\|T_s\|r_{cc}P_0\|TS)$ needs $2T_p + T_{e_1}$. After receiving all the *Data_Rep* of HID$_i$, $(1 \leq i \leq n)$, the computation of the authenticity and integrity of n *Data_Rep* based on batch verification involves $(n+2)T_p$. To compute $k_i^{'} = H_1(\hat{e}(PK_i, sk_{fd}r_{fd}r_iP_0))$, $C = \prod_{i=1}^{n}(C_i \cdot g^{-k_i^{'}}) \cdot H(T_s)^{\phi_0}\ mod\ N^2$ and $\sigma = sk_{fd}H_2(C\|ID_{fd}\|ID_{cc}\|T_s\|r_{fd}P_0\|TS)$, $(T_p + T_{e_2})$, $((n+1)T_{m_Z} + 2T_{e_Z})$ and T_{e_1} are needed respectively. In PDAF, the computation costs for each hybrid IoT device is $2(T_p + T_{e_2} + T_{e_Z} + T_{e_1})$. In fact, the computation costs for the secret key $k_i = H_1(\hat{e}(PK_{cc}, sk_ir_ir_{cc}P_0))$, $k_i^{'} = H_1(\hat{e}(PK_{fd}, sk_ir_ir_{fd}P_0))$ involves $2(T_p + T_{e_2})$. To protect private information, HID$_i$ needs $2T_{e_Z}$ computation costs for the ciphertext $C_i = g^{m_i+k_i+k_i^{'}}H(T_s)^{\phi_i}\ mod\ N^2$. To compute $\sigma_i = sk_iH_2(C_i\|ID_i\|ID_{fd}\|T_s\|r_iP_0\|TS)$, one T_{e_1} is needed. We represent the computation costs in Table 1.

Table 1. The computation cost of PDAF.

	Computation Costs
CC	$3T_p + 2T_{e_1} + T_{e_2} + T_{pai}$
FD	$(n+5)T_p + (n+1)T_{m_Z} + 2T_{e_1} + 2T_{e_Z} + T_{e_2}$
HID$_i$	$2(T_p + T_{e_2} + T_{e_Z} + T_{e_1})$

For the comparison with PDAF, in the following, we consider a traditional scheme, where all IoT devices blinded data C_i are not aggregated into a ciphertext C by the fog device. Under this setting, for n IoT device data, the total computation cost of the control center will increase by $(n-1)T_{pai}$ over the PDAF. The computation comparison is shown in Figure 3. Obviously, our PDAF scheme largely reduces the computation cost for the control center.

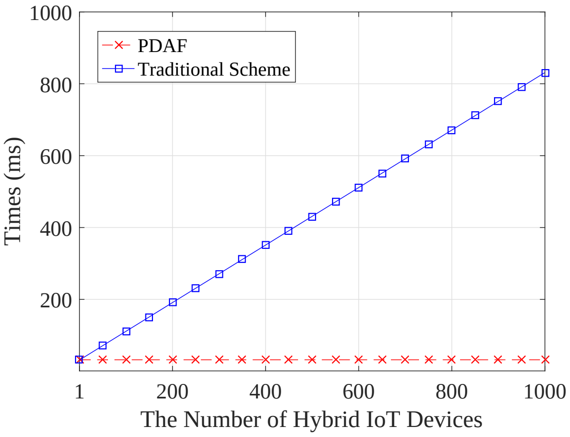

Figure 3. The computation cost comparison.

In addition, in the security model of paper [10], a trusted third party is considered because the control center and fog devices are honest-but-curious which may be affected by malicious attacks. Based on the trusted third party, the security of the system is guaranteed, but the communication and computation overhead is high. In [30], although there is not a trusted third party, we find that the control center may be affected by undetected malwares and hence violates a single user's data. It is possible to obtain sensitive information based on the private key λ, and the data aggregation scheme based on Paillier homomorphic encryption cannot completely protect sensitive information because the control center has the private key λ. In our proposed scheme, it is worth mentioning that the third-party trusted authority is not considered. In fact, the control center and fog device in PDAF are also honest-but-curious, but there is no risk of privacy leakage similar to [30].

5.2. Communication Overhead

In PDAF, we respectively denote the communication overhead of control center to fog devices (CC-to-FD), fog device to hybrid IoT devices (FD-to-HID), hybrid IoT devices to fog device (HID-to-FD) and fog device to control center (FD-to-CC) by l_{cf}, l_{fh}, l_{hf}, and l_{fc}. In addition, then, we define the size of each identity as 2 bytes, 4 bytes for T_s or time stamp TS, the length of the Paillier ciphertext is 2048 bits. Let G_1 be a 160-bit elliptic curve and the length of the signature is 160 bits. Firstly, in the control center to fog device communication, the length of $Data\_Req = \{ID_{cc}, ID_{fd}, T_s, r_{cc}P_0, TS, \sigma_{cc}\}$ is 52 bytes, that is $l_{cf} = 52$. In the fog device to hybrid IoT device communication, the $Data\_Req$ packet is of the form $\{ID_{fd}, ID_{cc}, T_s, r_{fd}P_0, r_{cc}P_0, TS, \sigma_{cc}\}$ and $l_{fh} = 72$. In the hybrid IoT device to fog device communication, the data collection request response $Data\_Rep$ of HID$_i(1 \leq i \leq n)$ contains $C_i, ID_i, ID_{fd}, T_s, r_iP_0, TS, \sigma_i$ and it length $l_{hf} = 308$ bytes. To reduce the communication overhead, the aggregated signature and ciphertext are sent to the control center by the fog device, which only need 275 bytes. The response message is of the form $\{C, ID_{cc}, ID_{fd}, T_s, \{r_iP_0\}_{1<i<n}, TS, \sigma\}$ and the size is $l_{fc} = 288 + 20n$ bytes where n is the number of hybrid IoT device. The communication overhead is listed in Table 2. Alternatively, if the traditional scheme is adopted, for n IoT device data, the length of l_{fc} will increase to $288 + 256n$ bytes. As shown in Figure 4, we further show the change of the communication overhead with the hybrid IoT devices number n. It is shown that the PDAF scheme obviously reduces bandwidth usage and communication overhead for the FD-to-CC communication.

In summary, the proposed PDAF approach is privacy-preserving and efficient in terms of the computation cost and communication overhead.

Table 2. The communication overhead of PDAF.

	Communication Overhead (Bytes)
l_{cf}	52
l_{fh}	72
l_{hf}	308
l_{fc}	$288 + 20n$

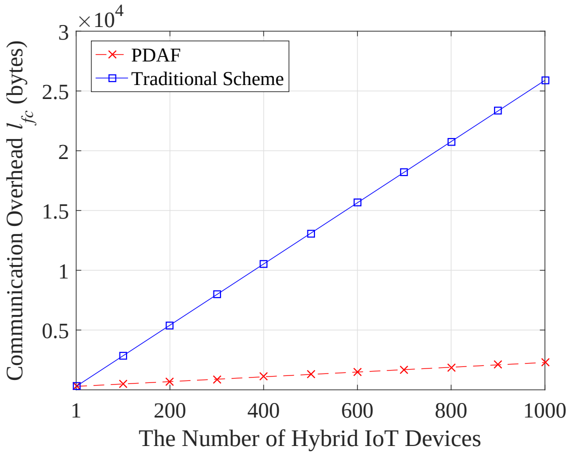

Figure 4. The communication overhead comparison.

6. Conclusions

In this paper, we have proposed a privacy-preserving data aggregation scheme based on the Paillier homomorphic encryption in fog computing and called PDAF. The idea realizes many security requirements such as privacy protection, non-repudiation, and unforgeability. The data aggregation technology based on homomorphic encryption not only can effectively protect the privacy of hybrid IoT devices but also can reduce the communication overhead of the system and improve the work efficiency of control centers and fog nodes. To improve the efficiency of data integrity checking, an efficient batch verification technology in use. In addition, blinding factor technology is also applied to our scheme, which makes the idea has better fault tolerance. Through analyzation of security and performance, the proposed scheme is reliable and efficient.

Author Contributions: Formal analysis, Y.Z., J.Z., D.Z., K.D., F.R. and X.Z.; Methodology, Y.Z. and D.Z.; Validation, Y.Z., J.Z., D.Z., K.D., F.R., X.Z. and J.S.; Writing-original draft, Y.Z., J.Z., K.D. and F.R.; Writing-review & editing, Y.Z., D.Z. and J.S.

Funding: This research was funded by National Key R&D Program of China under grant number 2017YFB0802000; National Natural Science Foundation of China under grant number 61772418, 61472472 and 61402366; Natural Science Basic Research Plan in Shaanxi Province of China under grant number 2018JZ6001 and 2015JQ6236. Yinghui Zhang is supported by New Star Team of Xi'an University of Posts and Telecommunications under grant number 2016-02.

Acknowledgments: We are grateful to the editors and referees for their invaluable suggestions for improving the paper.

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

References

1. Wang, Q.; Wang, C.; Ren, K.; Lou, W.; Li, J. Enabling public auditability and data dynamics for storage security in cloud computing. *IEEE Trans. Parallel Distrib. Syst.* **2011**, *22*, 847–859. [CrossRef]
2. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]

3. Zhang, Y.; Zheng, D.; Li, Q.; Li, J.; Li, H. Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing. *Secur. Commun. Netw.* **2016**, *9*, 3688–3702. [CrossRef]
4. Yang, L.; Han, Z.; Huang, Z.; Ma, J. A remotely keyed file encryption scheme under mobile cloud computing. *J. Netw. Comput. Appl.* **2018**, *106*, 90–99. [CrossRef]
5. Li, J.; Zhang, Y.; Chen, X.; Xiang, Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Comput. Secur.* **2018**, *72*, 1–12. [CrossRef]
6. Zhang, Y.; Yang, M.; Zheng, D.; Lang, P.; Wu, A.; Chen, C. Efficient and secure big data storage system with leakage resilience in cloud computing. *Soft Comput.* **2018**. [CrossRef]
7. Hosseinian-Far, A.; Ramachandran, M.; Slack, C.L. *Emerging Trends in Cloud Computing, Big Data, Fog Computing, IoT and Smart Living;* Springer: Cham, Switzerland, 2018; pp. 29–40.
8. Stergiou, C.; Psannis, K.E.; Kim, B.G.; Gupta, B. Secure integration of IoT and cloud computing. *Future Gener. Comput. Syst.* **2018**, *78*, 964–975. [CrossRef]
9. Zhang, Y.; Zheng, D.; Guo, R.; Zhao, Q. Fine-grained access control systems suitable for resource-constrained users in cloud computing. *Comput. Inf.* **2018**, *37*, 327–348. [CrossRef]
10. Lu, R.; Heung, K.; Lashkari, A.H.; Ghorbani, A.A. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT. *IEEE Access* **2017**, *5*, 3302–3312. [CrossRef]
11. Yannuzzi, M.; Milito, R.; Serral-Gracià, R.; Montero, D.; Nemirovsky, M. Key ingredients in an IoT recipe: Fog computing, cloud computing, and more fog computing. In Proceedings of the IEEE 19th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), Athens, Greece, 1–3 December 2014; pp. 325–329.
12. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the Internet of Things. In Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, New York, NY, USA, 17 August 2012; pp. 13–16. [CrossRef]
13. Shen, J.; Wang, C.; Li, T.; Chen, X.; Huang, X.; Zhan, Z.H. Secure data uploading scheme for a smart home system. *Inf. Sci.* **2018**, *453*, 186–197. [CrossRef]
14. Zhang, Y.; Zheng, D.; Deng, R.H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control. *IEEE Internet Things J.* **2018**, *5*, 2130–2145. [CrossRef]
15. Shen, J.; Gui, Z.; Ji, S.; Shen, J.; Tan, H.; Tang, Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *J. Netw. Comput. Appl.* **2018**, *106*, 117–123. [CrossRef]
16. Zhang, Y.; Chen, X.; Li, J.; Li, H. Generic construction for secure and efficient handoff authentication schemes in EAP-based wireless networks. *Comput. Netw.* **2014**, *75*, 192–211. [CrossRef]
17. Han, Q.; Zhang, Y.; Chen, X.; Li, H.; Quan, J. *Efficient and Robust Identity-Based Handoff Authentication in Wireless Networks;* Springer: Berlin/Heidelberg, Germany, 2012; pp. 180–191.
18. Zhang, Y.; Chen, X.; Li, H.; Cao, J. Identity-based construction for secure and efficient handoff authentication schemes in wireless networks. *Secur. Commun. Netw.* **2012**, *5*, 1121–1130. [CrossRef]
19. Wang, C.; Shen, J.; Liu, Q.; Ren, Y.; Li, T. A novel security scheme based on instant encrypted transmission for Internet of Things. *Secur. Commun. Netw.* **2018**, *2018*, 3680851. [CrossRef]
20. Jhaveri, R.H.; Patel, N.M.; Zhong, Y.; Sangaiah, A.K. Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. *IEEE Access* **2018**, *6*, 20085–20103. [CrossRef]
21. Zhang, Y.; Li, J.; Chen, X.; Li, H. Anonymous attribute-based proxy re-encryption for access control in cloud computing. *Secur. Commun. Netw.* **2016**, *9*, 2397–2411. [CrossRef]
22. Bhuiyan, M.Z.A.; Wu, J.; Wang, G.; Cao, J. Sensing and decision making in cyber-Physical systems: The case of structural event monitoring. *IEEE Trans. Ind. Inf.* **2016**, *12*, 2103–2114. [CrossRef]
23. Shu, J.; Jia, X.; Yang, K.; Wang, H. Privacy-preserving task recommendation services for crowdsourcing. *IEEE Trans. Serv. Comput.* **2018**. [CrossRef]
24. Shu, J.; Liu, X.; Jia, X.; Yang, K.; Deng, R.H. Anonymous privacy-preserving task matching in crowdsourcing. *IEEE Internet Things J.* **2018**, 5, 3068–3078. [CrossRef]
25. He, D.; Kumar, N.; Zeadally, S.; Vinel, A.; Yang, L.T. Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries. *IEEE Trans. Smart Grid* **2017**, *8*, 2411–2419. [CrossRef]
26. Zhang, Y.; Zhao, J.; Zheng, D. Efficient and privacy-aware power injection over AMI and smart grid slice in future 5G networks. *Mob. Inf. Syst.* **2017**, *2017*, 3680671. [CrossRef]

27. Zhang, Y.; Li, J.; Zheng, D.; Li, P.; Tian, Y. Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. *J. Netw. Comput. Appl.* **2018**. [CrossRef]
28. Jia, W.; Zhu, H.; Cao, Z.; Dong, X.; Xiao, C. Human-factor-aware privacy-preserving aggregation in smart grid. *IEEE Syst. J.* **2014**, *8*, 598–607. [CrossRef]
29. Stojmenovic, I. Fog computing: A cloud to the ground support for smart things and machine-to-machine networks. In Proceedings of the Australasian Telecommunication Networks and Applications Conference (ATNAC), Southbank, VIC, Australia, 26–28 November 2014; pp. 117–122.
30. Mahmoud, M.; Saputro, N.; Akula, P.; Akkaya, K. Privacy-preserving power injection over a hybrid AMI/LTE smart grid network. *IEEE Internet Things J.* **2016**, *4*, 870–880. [CrossRef]
31. Mukherjee, M.; Matam, R.; Shu, L.; Maglaras, L.; Ferrag, M.A.; Choudhury, N.; Kumar, V. Security and privacy in fog computing: challenges. *IEEE Access* **2017**, *5*, 19293–19304. [CrossRef]
32. Zhang, Y.; Chen, X.; Li, J.; Wong, D.S.; Li, H.; You, I. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. *Inf. Sci.* **2017**, *379*, 42–61. [CrossRef]
33. Zhang, Y.; Wu, A.; Zheng, D. Efficient and privacy-aware attribute-based data sharing in mobile cloud computing. *J. Ambient Intell. Hum. Comput.* **2018**, 9, 1039–1048. [CrossRef]
34. Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; pp. 223–238.
35. Xu, J.; Wei, L.; Zhang, Y.; Wang, A.; Zhou, F.; Gao, C.Z. Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. *J. Netw. Comput. Appl.* **2018**, *107*, 113–124. [CrossRef]
36. Gao, C.z.; Cheng, Q.; He, P.; Susilo, W.; Li, J. Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. *Inf. Sci.* **2018**, *444*, 72–88. [CrossRef]
37. Shen, H.; Zhang, M.W. A Privacy-preserving multilevel users' electricity consumption aggregation and control scheme in smart grids. *J. Cryptol. Res.* **2016**, *3*, 171–191.
38. Zhang, Y.; Shu, J.; Liu, X.; Li, J.; Zheng, D. Security analysis of a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. *IEEE Internet Things J.* **2018**. [CrossRef]
39. Lai, X.; Zou, W.; Xie, D.; Li, X.; Fan, L. DF relaying networks with randomly distributed interferers. *IEEE Access* **2017**, *5*, 18909–18917. [CrossRef]
40. Zhang, Y.; Lang, P.; Zheng, D.; Yang, M.; Guo, R. A secure and privacy-aware smart health system with secret key leakage resilience. *Secur. Commun. Netw.* **2018**, *2018*, 7202598. [CrossRef]
41. Fan, L.; Lei, X.; Yang, N.; Duong, T.Q.; Karagiannidis, G.K. Secrecy cooperative networks with outdated relay selection over correlated fading channels. *IEEE Trans. Veh. Technol.* **2017**, *66*, 7599–7603. [CrossRef]
42. Fan, L.; Lei, X.; Yang, N.; Duong, T.Q.; Karagiannidis, G.K. Secure multiple amplify-and-forward relaying with cochannel interference. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1494–1505. [CrossRef]
43. Tan, W.; Xie, D.; Xia, J.; Tan, W.; Fan, L.; Jin, S. Spectral and energy efficiency of massive MIMO for hybrid architectures based on phase shifters. *IEEE Access* **2018**, *6*, 11751–11759. [CrossRef]
44. Bhuiyan, M.Z.A.; Wu, J.; Wang, G.; Chen, Z.; Chen, J.; Wang, T. Quality-guaranteed event-sensitive data collection and monitoring in vibration sensor networks. *IEEE Trans. Ind. Inf.* **2017**, *13*, 572–583. [CrossRef]
45. Gershenfeld, N.; Krikorian, R.; Cohen, D. The Internet of Things. *Sci. Am.* **2004**, *291*, 76–81. [CrossRef] [PubMed]
46. Zhou, H.; Chen, J.; Zhang, Y.Y.; Dang, L.J. A multidimensional data aggregation scheme in multilevel network in smart grid. *J. Cryptol. Res.* **2017**, *4*, 114–132.
47. Zhang, Y.; Deng, R.H.; Liu, X.; Zheng, D. Blockchain based efficient and robust fair payment for outsourcing services in cloud computing. *Inf. Sci.* **2018**, *462*, 262–277. [CrossRef]
48. Zhang, Y.; Deng, R.H.; Shu, J.; Yang, K.; Zheng, D. TKSE: trustworthy keyword search over encrypted data with two-side verifiability via blockchain. *IEEE Access* **2018**, *6*, 31077–31087. [CrossRef]
49. Zhang, Y.; Deng, R.H.; Liu, X.; Zheng, D. Outsourcing service fair payment based on blockchain and its application in cloud computing. *IEEE Trans. Serv. Comput.* **2018**. [CrossRef]
50. Chen, X.; Li, J.; Weng, J.; Ma, J.; Lou, W. Verifiable computation over large database with incremental updates. *IEEE Trans. Comput.* **2016**, *65*, 3184–3195. [CrossRef]
51. Chen, W.; Lei, H.; Qi, K. Lattice-based linearly homomorphic signatures in the standard model. *Theor. Comput. Sci.* **2016**, *634*, 47–54. [CrossRef]

52. Lin, Q.; Yan, H.; Huang, Z.; Chen, W.; Shen, J.; Tang, Y. An ID-based linearly homomorphic signature scheme and its application in blockchain. *IEEE Access* **2018**, *6*, 20632–20640. [CrossRef]
53. Chen, X.; Li, J.; Huang, X.; Ma, J.; Lou, W. New publicly verifiable databases with efficient updates. *IEEE Trans. Dependable Secure Comput.* **2015**, *12*, 546–556. [CrossRef]