IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 November 2022, accepted 29 November 2022, date of publication 1 December 2022,
date of current version 23 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3226245

RESEARCH ARTICLE

Federated Learning-Based Privacy-Preserving Data Aggregation Scheme for IIoT

HONGBIN FAN[1,2,4], CHANGBING HUANG[1,3], AND YINING LIU[2], (Member, IEEE)

[1]College of Computer and Artificial Intelligence, Xiangnan University, Chenzhou 423000, China
[2]Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin 541004, China
[3]Affiliated Hospital (Clinical College), Xiangnan University, Chenzhou 423000, China
[4]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China

Corresponding author: Changbing Huang (huangchangbing234@163.com)

This work was supported in part by the Guangxi Key Laboratory of Trusted Software under Grant KX202048; in part by the Special Patient Positioning and Telemedicine Information Technology Research and Development Center of Chenzhou (Chen Caijiaozhi [2020] No. 35); in part by the Clinical Medical Technology Innovation Guidance Plan Project of Department of Science and Technology of Hunan Province under Grant 2021SK52201 and Grant 2018SK52007; in part by the Science and Technology Planning Project of Chenzhou Municipal Science and Technology Bureau under Grant lcyl2021098; in part by the Teaching Reform Research Project of Xiangnan University (XiaoFa [2022] No. 35 of XiangNan University, Serial No. 56); and in part by the General Scientific Research Project of Hunan Provincial Department of Education, Application research on automatic identification and classification of antler mushrooms based on deep learning, under Grant 20C1193.

ABSTRACT The Industrial Internet of Things (IIoT) is the key technology of Industry 4.0. The combination of machine learning and IIoT has spawned a thriving smart industry. Machine learning models are trained and predicted based on raw data that contains sensitive information, and data sharing leads to information leakage. Data security and privacy protection in IIoT face serious challenges. Therefore, we propose a federated learning-based privacy-preserving data aggregation scheme (FLPDA) for IIoT. Data aggregation to protect individual user model changes in federated learning against reverse analysis attacks from industry administration centers. Each round of data aggregation uses the PBFT consensus algorithm to select an IIoT device from the aggregation area as the initialization and aggregation node. Paillier cryptosystem and secret sharing are combined to realize data fault tolerance and secure sharing. Security analysis and performance evaluation show that the scheme can effectively protect data privacy and resist various attacks. It has lower communication, computational, and storage overhead than existing schemes.

INDEX TERMS Federated learning, IIoT, PBFT, privacy-preserving.

I. INTRODUCTION

Industrial devices are interconnected through the Internet of Things to form the Industrial Internet of Things (IIoT), becoming one of the key technologies to achieve Industry 4.0. With the rapid development of wireless communication, the wide application of big data, artificial intelligence (AI), 5G, and other technologies, IIoT is becoming intelligent, which has dramatically improved industrial productivity and efficiency [1]. The Industrial Internet of Things has emerged a variety of advanced mobile devices, such as smart gateways, smart watches, smartphones, etc. The industrial data generated by IIoT is developed by AI through machine learning technology and applied to various fields such as smart healthcare, autonomous driving, smart cities, smart homes, and live games [2], [3], [4]. Smart devices generate industrial data containing sensitive information transmitted, shared, and stored in IIot [5]. For example, in autonomous driving, smart devices provide users with navigation and emergency avoidance by sensing road condition information and real-time vehicle status [6]. If data security and user privacy are not guaranteed, attackers will tamper with private data, cause traffic network accidents, and endanger personal safety. Therefore, it is crucial to ensure the data security and privacy protection of smart devices in IIoT.

The associate editor coordinating the review of this manuscript and approving it for publication was Theofanis P. Raptis.

Machine learning has advantages such as real-time prediction, improved industrial automation, and saved time and cost. The combination of machine learning and IIoT has spawned a booming intelligent industry. Traditional machine learning often requires collecting large amounts of raw data from IIoT devices (such as gateways) to train, requiring all IIoT devices to upload data to a central server and then train learning models. The rapid development of machine learning brings convenience to people, but also carries significant security risks. The training and prediction of machine learning models are based on raw data containing sensitive information, and data sharing will lead to information leakage. Without access to rich shared data, it isn't easy to train high-precision models. Security and privacy concerns about machine learning have become stumbling blocks. How to make data be used in real-time without disclosing its privacy has become a problem that the industrial Internet of Things must solve.

Inspired by this issue, Federated Learning (FL) is proposed [7]. It lets devices in the industrial Internet of Things collaborate to learn a common model by exchanging model parameters with a central server rather than raw data. Training data in federated learning is still stored locally, eliminating the need to access local data directly, and reducing the risk of privacy breaches. FL aggregates local model parameters from many IIoT devices to train global models, and model accuracy will be significantly improved [8]. During the transmission of federated learning models, adversaries can use the correlation between model output and sensitive data features to predict sensitive information based on background information and published models, thereby increasing the risk of privacy information leakage [9]. A single user usually only has a small amount of data to train the local model, and FL compares the trained and untrained local model, easily obtaining the trained datasets containing sensitive information. Thus, FL is vulnerable to reverse analysis attacks. Therefore, it is a challenge to design FL solutions that meet the requirements of individual privacy and information security.

To solve the above problems, we propose a federated learning-based privacy-preserving data aggregation scheme (FLPDA) for IIoT, which combines federated learning with secret sharing to aggregate data. In this scheme, each round of federated learning elects initializing and aggregating nodes through the PBFT consensus algorithm, which changes the dependence of the existing scheme on trusted entities and dramatically reduces the risk of information leakage. Data aggregation is an effective method to protect data privacy and reduce communication overhead [10], [11], [12], which is used to protect the changes of individual user model in FL and prevent reverse analysis attacks from the central server. Paillier cryptosystem and secret sharing are combined to achieve fault tolerance, data security, and sharing.

The main contributions of this paper are as follows:

(1) A federated learning-based privacy-preserving data aggregation scheme for IIoT is proposed. Through the PBFT consensus algorithm, one of the smart devices in IIoT is selected as the initialization and aggregation node, which does not rely on trusted authorities or trusted third parties.

(2) Data aggregation is adopted to protect model change of industrial devices in FL and resist the reverse analysis attack from the industry management center. Secret sharing is applied to share IIoT data while achieving fault tolerance.

(3) The lower overhead of computation, communication, and storage in FLPDA means that the system has better efficiency and higher execution speed, which is very suitable for data aggregation in IIoT.

The remainder of this paper is organized as follows: The related works are discussed in Section II. Sections III and IV present the relevant preliminaries and the proposed system model, respectively. In Section V, FLPDA is described in detail. Security analysis and performance evaluation are carried out in Sections VI and VII, respectively. Section VIII concludes this paper.

II. RELATED WORK

In recent years, the research on the privacy protection of federated learning and its application in IIoT has attracted extensive attention in the academic community.

Ma et al. [13] proposed a privacy-preserving multi-party framework for federated learning. Bilinear aggregation signatures are used to verify the correctness of the ag-gregation results, and all participants participate in the verification. Therefore, the computational cost increases significantly with the number of participants. In [14], the authors combine the Harn-Gong key with data aggregation to propose a machine learning data aggregation scheme with non-interactive keys. The results show that the scheme has a private data masking function. However, the scheme relies on the trusted authority to distribute the keys. Authors in [15] present a hybrid privacy-preserving federated learning scheme, which combines secure multi-party computation with differential privacy to reduce the noise injection that increases with the number of participants without sacrificing privacy. In [16], a privacy-preserving federated neural network learning scheme is proposed to solve the problem of neural network evaluation and privacy-preserving training in an N-square federated learning environment. Bonawitz et al. [17] designed a federated learning secure aggregation scheme for high-dimensional data, which allows the central server to compute the sum of data vectors from mobile devices securely with communication efficiency and fault robustness. Song et al. [18] proposed an efficient secret-sharing privacy-preserving FL data aggregation mechanism, which can aggregate user-trained models without revealing user models, with efficient fault tolerance and resistance to reverse attacks. Scheme [15], [16], [17] has high computation and communication costs, and cannot resist replay attacks. Scheme [18] also fails to defend against replay attacks.

Tian et al. [19] proposed a blockchain-based machine learning framework for IIoT. The scheme builds a new smart contract, which uses the aggregation strategy to verify and aggregate the model parameters to ensure the accuracy of the decision tree model. But miners are assumed to be honest and trustworthy nodes.

All the above schemes proposed a theoretical framework, but did not design specific federal learning methods for privacy protection.

Kong et al. [20] proposed a privacy-preserving model aggregation scheme based on a federated learning navigation framework. A homomorphic threshold cryptosystem combines the skip list and the bounded Laplace mechanism to protect the locally trained model updates. Zhou et al. [21] proposed a blockchain-based federated data sharing scheme. A federated extreme gradient boosting learning algorithm is constructed to solve the data isolation problem, and a data sharing mechanism is designed to ensure secure on-demand control data sharing. Scheme [20] relies on the trusted authority (TA), and scheme [21] assumes that the Key generation center (KGC) is the trusted entity. In fact, a trusted entity does not exist, and there is a risk of information source leakage, so it is not practical.

We propose a scheme combining PBFT, data aggregation, and federated learning. It solves the problem that existing data aggregation solutions rely on trusted entities, while resisting the reverse analysis attack problem of federated learning solutions.

III. PRELIMINARIES

A. FEDERATED LEARNING

FL is a distributed machine learning model. The model is trained on the user side to protect the user's privacy, and then the model update is transmitted to the central manager for aggregation. Raw data remains in local storage. During local model training, the central manager can access all local model updates and share model data with other servers in the aggregation area. The global model in the central manager is then updated and shared back to the local device for further training [22].

FL is a typical example of machine learning and analysis on mobile wearable devices through 5G and later wireless networks, which have been deployed to sensitive healthcare applications [23].

B. PBFT

The practical byzantine fault tolerance (PBFT) consensus algorithm is a distributed voting mechanism. Its purpose is to solve the consensus problem in an N-nodes network with F concurrent failed nodes, where N satisfies $N > 3F + 1$ [24].

PBFT is divided into three processes: pre-prepare, prepare, and commit, which solves the problem of General Byzantine [25].

C. SECRET SHARING

Secret sharing is an entirely homomorphic scheme, which uses Shamir technology to split a secret into L parts and allocate them to different members. If an opponent steals part of the system, it can only gain part of the secret. It can obtain the whole secret only if it gets at L pieces of the secret [26].

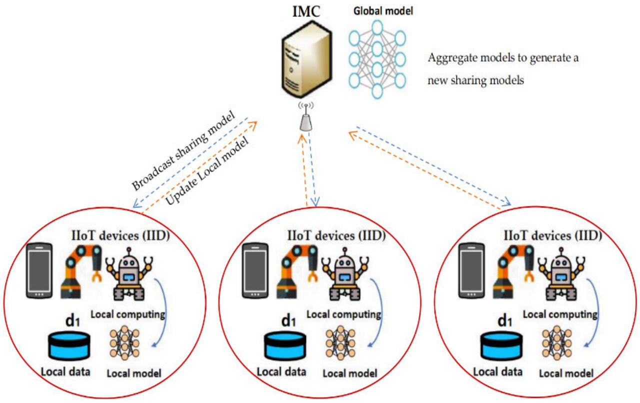

FIGURE 1. System model.

The following polynomial was chosen to split a secret.

$$E(y) = \alpha + p_1 y + p_2 y^2 + \cdots + p_{L-1} y^{L-1} \tag{1}$$

where $\alpha$is a secret, and L is a threshold value.

The following formula can be obtained by Lagrange interpolation polynomial

$$E(y) = \sum\nolimits_{k=1}^{L} \left(\sum\nolimits_{j=1, j\neq k}^{L} \frac{y_j - y}{y_j - y_k}\right) E(y_k)$$
$$\gamma_{y_j} = \prod\nolimits_{k\neq j}^{L} \frac{y_k}{y_k - y_j} \tag{2}$$

Then a is calculated as follows:

$$\sum\nolimits_{j=1}^{L} E(y_j)\gamma_{y_j} = E\ (0) \tag{3}$$

IV. SYSTEM MODEL

A. COMMUNICATION MODEL

As shown in Figure 1, the hierarchical structure of industrial data communication is composed of IIoT devices (IID) and Industrial Management Center (IMC). The following presents the details of each component.

(1) IID: Each user is equipped with a wearable smart device for industrial data collection. One user is equal to an IID. IIDs simultaneously and regularly collect IIoT data. P2P communication is used between all IIDs in each aggregation area. Each aggregation area adopts PBFT consensus algorithm to select an IID from all IIDs as system initialization and data aggregation node (SN). Sometimes IIDs may stop reporting or reset later due to failure. IID is assumed to be honest but curious.

(2) IMC: IMC reads aggregated real-time IIoT data.

B. ADVERSARY MODEL

In our model, IMC and IID are semi-trusted. IMC or IID does not tamper arbitrarily with its industrial data, but it may want to gain access to other people's private industrial information and sell it to interested entities.

TABLE 1. Notations.

Symbol	Quantity
g_0, g_1	A generator of G
IMC	Industrial Management Center
$\mathrm{IID_j}$	The j-th IIoT device
SN	System initialization and data aggregation node
d_j	Industrial data of $\mathrm{IID_j}$
N	Number of smart devices in the aggregation area
H_1, H_2	Hash functions: H_1, H_2: $\{0,1\}^* \rightarrow G$
$\Vert$	Concatenation operation

Internal attackers may conspire to access other users' industrial sensitive private information. An external attacker may attempt to impersonate a legitimate entity (i.e., a smart industrial device in the aggregation area) and send relevant data on its behalf. In addition, external eavesdroppers may eavesdrop on network traffic to obtain industrial data and attempt to modify and forward it.

C. DESIGN GOALS

(1) Data security. It can resist various attacks. Even if the aggregated ciphertext of IIoT data collected by smart devices is intercepted, the IIoT data of a single smart device cannot be recovered.

(2) Privacy. Industrial data can be securely aggregated against internal and external attacks. No entity can obtain the industrial data of a single smart device.

(3) Fault tolerance. If the smart device is not able to collect industrial data due to external malicious damage or failure, the utility of the system is significantly compromised. Even if some smart devices cannot collect or send industrial data, the system can still effectively aggregate the data of IIoT from other smart devices.

V. THE PROPOSED SCHEME

In this section, we introduce a federated learning-based privacy-preserving data aggregation scheme for IIoT. The notations are listed in Table 1.

A. INITIALIZATION

Suppose each aggregation area has N SDs recorded as a set $P_g = \{\mathrm{SD}_1, \mathrm{SD}_2, \ldots, \mathrm{SD_N}\}$. Some users do not participate in IIoT data aggregation because of specific concerns or because IIDs may be malfunctioning. It is assumed that there are at least L SDs online and participate in aggregation, these IIDs constitute $P_{on} \subseteq P_g$. Through the PBFT consensus algorithm, each round of data aggregation selects an IID from the data aggregation area P_g as system initialization and data aggregation node (SN).

SN runs Paillier cryptosystem to generate (q, g_0, G_1, G_2, e), $e : G_1 \times G_1 \rightarrow G_2$, G_1 and G_2 are cyclic groups of order p, calculates public-private key pairs $\{(N, g), (\lambda, \mu)\}$, $g_0 \in G_1, g_1 \in Z^*_{N^2}$.

SN chooses three hash functions H_0, H_1 and H_2, where$H_0 : \{0, 1\}^* \rightarrow Z^*_N, H_1, H_2 : \{0, 1\}^* \rightarrow G_1$.

SN publishes the parameter $\{q, g_0, g_1, G_1, G_2, e, N, H_0, H_1, H_2\}$.

B. ROUND 0 (ADVERTISE KEYS)

IID:

(1) Request IMC to update data.

(2) $\mathrm{IID_j}$ selects $s_j \in Z^*_q$ as the private key and computes the corresponding public key $P_j = s_j \cdot g_0$, then it sends P_j to IMC.

IMC:

(1) IMC collects at least L messages from $\mathrm{IID_j}$ in the previous round.

(2) Make sure the number N of IIDs, the threshold value L.

(3) Broadcast list of received public keys to IIDs in P_{on}.

C. ROUND 1 (SHARES GENERATION)

IID:

(1) Receive global parameters broadcasted by the server. Verify that $|P_{on}| \geq L$.

(2) Generate secret shares, $\mathrm{IID_j}$ generates its polynomial $E(y_j) = \alpha + p_1 y_j + p_2 y_j^2 + \cdots + p_{L-1} y_j^{L-1}$, $\gamma_{y_j} = \prod_{k \neq j}^{L} \frac{y_k}{y_k - y_j}$, then sends $Ts \Vert E(y_j)\gamma_{y_j}$ to IMC.

IMC:

(1) Forward received shares to IIDs in P_{on}.

D. ROUND 2 (CIPHERTEXT GENERATION AND VERIFICATION SIGNATURE)

IID:

(1) $\mathrm{IID_j}$ generates IIoT data d_j at timestamp Ts, and computes H_0 (Ts), then selects $r_j \in Z^*_N$ to generate ciphertext:

$$C_j = g_1^{d_j} \times r_j^N \times H_0(Ts)^{E(y_j)\gamma_{y_j}} mod\ N^2$$

(2) $\mathrm{IID_j}$ generates signature $\sigma_j = s_j \cdot H_2(C_j \Vert P_j \Vert H_1(Ts \Vert E(y_j)\gamma_{y_j}))$.

(3) $\mathrm{IID_j}$ sends $C_j \Vert P_j \Vert H_1(Ts \Vert E(y_j)\gamma_{y_j}) \Vert \sigma_j$ to IMC and SN.

IMC:

(1) After receiving $C_j \Vert P_j \Vert H_1(Ts_j \Vert E(y_j)\gamma_{y_j}) \Vert \sigma_j$, IMC batch verification signature

$$\begin{aligned} & e\left(\sum_{j=1}^{L} \sigma_j, g_0\right) \\ & = e\left(\sum_{j=1}^{L} s_j \cdot H_2\left(C_j \Vert P_j \Vert H_1\left(Ts_j \Vert E\left(y_j\right)\gamma_{y_j}\right)\right), g_0\right) \\ & = \prod_{j=1}^{L} e\left(s_j \cdot H_2\left(C_j \Vert P_j \Vert H_1\left(Ts_j \Vert E\left(y_j\right)\gamma_{y_j}\right)\right), g_0\right) \\ & = \prod_{j=1}^{L} e(H_2(C_j \Vert P_j \Vert H_1(Ts_j \Vert E(y_j)\gamma_{y_j})), s_j \cdot g_0) \end{aligned}$$

(2) Forward batch signature verification results to SN.

E. ROUND 3 (CIPHERTEXT AGGREGATION AND SECRET RECONSTRUCTION)

IID:

(1) SN aggregates the ciphertext of all IIDs.

$$\begin{aligned} C &= \prod_{j=1}^{N} g_1^{d_j} \times r_j^N \times H_0(Ts)^{E(y_j)\gamma_{y_j}} \bmod \mathrm{N}^2 \\ &= g_1^{\sum_{j=1}^{N} d_j} \cdot r_j^N \times H_0(Ts)^{\sum_{j=1}^{L} E(y_j)\gamma_{y_j}} \bmod \mathrm{N}^2 \\ &= g_1^{\sum_{j=1}^{N} d_j} \cdot r_j^N \times H_0(Ts)^0 \bmod \mathrm{N}^2 \\ &= g_1^{\sum_{j=1}^{N} d_j} \cdot r_j^N \bmod \mathrm{N}^2 \end{aligned}$$

(2) SN sends C to IMC.

IMC:

(1) After the batch verification signature is passed, IMC arbitrarily chooses L shares of $E(y_j)\gamma_{y_j}$ from the received N shares of $E(y_j)\gamma_{y_j}$ to reconstruct the secret.

$$\alpha = E(0) = \sum_{j=1}^{L} E(y_j)\gamma_{y_j}.$$

$$\text{Let } \alpha = 0, \text{ so } \sum_{j=1}^{L} E(y_j)\gamma_{y_j} = 0.$$

F. ROUND 4 (CIPHERTEXT DECRYPTION)

IMC uses the private key (λ, μ) to decrypt C to obtain the aggregated the data of IIDs.

$$\begin{aligned} Dec(C) &= \frac{L(g^{(\sum_{j=1}^{N} d_j)\lambda} \bmod \mathrm{N}^2)}{L(g^{\lambda} \bmod \mathrm{N}^2)} \bmod \mathrm{N} \\ &= \sum_{j=1}^{N} d_j \end{aligned}$$

VI. SECURITY ANALYSIS

A. DATA INTEGRITY

FLPDA scheme adopts BLS short signature to sign private data and aggregate data of IIDs.

For the message $C_j \parallel P_j \parallel H_1(Ts_j \parallel E(y_j)\gamma_{y_j}) \parallel \sigma_j$ sent by $\mathrm{IID_j}$, IMC first checks P_j and $H_1(Ts_j \parallel E(y_j)\gamma_{y_j})$, and then verifies the integrity of the message by checking whether $e(\sum_{j=1}^{L} \sigma_j, g_0) = e(\sum_{j=1}^{L} s_j \cdot H_2(C_j \parallel P_j \parallel H_1(Ts_j \parallel E(y_j)\gamma_{y_j})), g_0)$ is established. Each element of the message is involved in validation, and any manipulation of the message results in unequal batch validation. Therefore, the integrity of the messages sent by $\mathrm{IID_j}$ can be verified by IMC.

B. PRIVACY-PRESERVATION

Attackers can be divided into internal attackers and external attackers. The internal attackers include IMC and IIDs in this aggregated area who seek to compromise the privacy of other IIDs. External attackers are entities that are not in this aggregated area.

Theorem 1: FLPDA scheme is resistant to external attacks, i.e., it is computationally infeasible for an external adversary to obtain d_j from C_j.

Proof: When an external attacker infiltrates an IID, the ciphertext $C_j = g_1^{d_j} \times r_j^N \times H_0(Ts)^{E(y_j)\gamma_{y_j}} \bmod N^2$ sent by the IID can be obtained. Since the attacker does not know the decryption key λ and the shared keys of other L-1 users. Therefore, an external attacker cannot obtain the plaintext.

Theorem 2: FLPDA scheme is resistant to internal attacks, i.e., it is computationally infeasible for an internal opponent (IID or IMC) to extract d_j from C_j.

Proof: The other user's $\mathrm{IID_k}$ $(k \neq j)$ could not successfully extract d_j from C_j,because he doesn't know $H_0(Ts)^{E(y_j)\gamma_{y_j}}$. Even if the malicious IIDs obtained $H_0(Ts)^{E(y_j)\gamma_{y_j}}$ of $\mathrm{IID_j}$, they did not know the decryption key λ by paillier's encryption algorithm, so they still could not obtain the plaintext of $\mathrm{IID_j}$. IMC does not know $H_0(Ts)^{E(y_j)\gamma_{y_j}}$ of $\mathrm{IID_j}$ and cannot derive the real-time data of $\mathrm{IID_j}$, only the aggregated data of all IIDs can be obtained. Therefore, FLPDA scheme can resist internal attacks.

Theorem 3: FLPDA scheme can resist the reverse analysis attack.

Proof: Suppose IMC is a potential adversary, trying to obtain the individual data of each device. After IMC receives the aggregated ciphertext C sent by SN, the decryption gets $\sum_{j=1}^{N} d_j$ via (λ, μ). IMC cannot obtain the ciphertext C_j of a single device IID, so it cannot obtain d_j. IMC only obtains the aggregated data of all IIDs, but does not know the single data of each IID. Therefore, FLPDA scheme can resist the reverse analysis attack.

Theorem 4: FLPDA scheme can resist the conspiracy attack.

Proof: If SN gets the decrypted key from IMC and tries to acquire the plaintext of $\mathrm{IID_j}$, the privacy of $\mathrm{IID_j}$ can still be preserved because they don't know $H_0(Ts)^{E(y_j)\gamma_{y_j}}$. Moreover, if at least L IIDs conspire, they can get $\sum_{j=1}^{L} E(y_j)\gamma_{y_j}$. Because they don't know the decryption key λ, they still can't get the data of a single IID.

C. FAULT TOLERANCE

Some devices may malfunction and do not send industrial data to SN at all. As SN only knows which group an IID belongs to according to β_j. IMC uses $H_1(Ts_j \parallel E(y_j)\gamma_{y_j})$ to find the malfunctioning $\mathrm{IID_j}$, while masking the IID's identity.

First, IMC compares this group of hash tables constituted by $H_1(Ts_j \parallel E(y_j)\gamma_{y_j})$ with other complete groups to find the malfunctioning IID. Then, selects an IID from other groups with the same hash value $H_1(Ts_j \parallel E(y_j)\gamma_{y_j})$ to replace $\mathrm{IID_j}$. Therefore, if there is a malfunctioning $\mathrm{IID_j}$, we shouldn't consider $\mathrm{IID_j}$'s data. IMC arbitrarily chooses L shares of $E\left(y_j\right)\gamma_{y_j}$ from the received $(N\text{-}1)$ shares of $E(y_j)\gamma_{y_j}$ to reconstruct the secret.

Let's assume $\mathrm{IID_{j'}}$ $(1 \leq j' \leq L)$ has failed to transmit $d_{j'}$ to SN, then SN aggregates the aggregated ciphertext of IIDs.

$$C = \prod_{j=1, j\neq j'}^{N-1} g_1^{d_j} \times r_j^N \times H_0(Ts)^{E(y_j)\gamma_{y_j}} \bmod \mathrm{N}^2$$

TABLE 2. Feature comparison.

Features	[15]	[17]	[18]	[20]	[21]	FLPDA
Privacy preservation	√	√	√	√	√	√
Fault Tolerance	×	√	√	√	×	√
No Trusted Party	×	√	√	×	×	√
Round-efficient	×	√	√	×	×	√
Dropout	×	√	√	√	×	√
Resist reverse attacks	×	×	√	×	×	√
No Expensive Operations	×	×	√	×	√	√
Resilience against reply attacks	×	×	×	√	×	√
Collusion resistance	√	√	√	√	√	√

TABLE 3. Computational overhead.

Algorithm	[18]	[20]	FLPDA
Key generation	2N	2N	N
Encryption	N	6N	N
Decryption	1	1	1
Signature generation	N	N	N
Signature verification	N	N	1
Key agreement	2N	2N	0
Secret sharing	N	2N	N
Secret reconstruction	1	1	1

$$
\begin{aligned}
&= g_1^{\sum_{j=1,j\neq j'}^{N-1} d_j} \cdot r_j^N \times H_0(Ts)^{\sum_{j=1}^{L} E(y_j)\gamma_{y_j}} \bmod \mathrm{N}^2 \\
&= g_1^{\sum_{j=1,j\neq j'}^{N-1} d_j} \cdot r_j^N \times H_0(Ts)^N \bmod \mathrm{N}^2 \\
&= g_1^{\sum_{j=1,,j\neq j'}^{N-1} d_j} \cdot (r_j \times H_0(Ts))^N
\end{aligned}
$$

IMC uses the private key (λ, μ) to decrypt C.

$$Dec(C) = \sum_{j=1,j\neq j'}^{N-1} d_j$$

IMC obtains the aggregated industrial data of all IIoT devices except $\mathrm{IID}_{j'}$. As a result, IMC can get the right aggregation results in this case, and thus our scheme achieves the fault-tolerant property.

D. FEATURE COMPARISON

In Table 2, the comparison between our scheme and other related schemes [15], [17], [18], [20], [21] shows that our scheme does not require any trusted entity, can resist all attacks, meets the privacy protection requirements, and realizes reverse attack resistance.

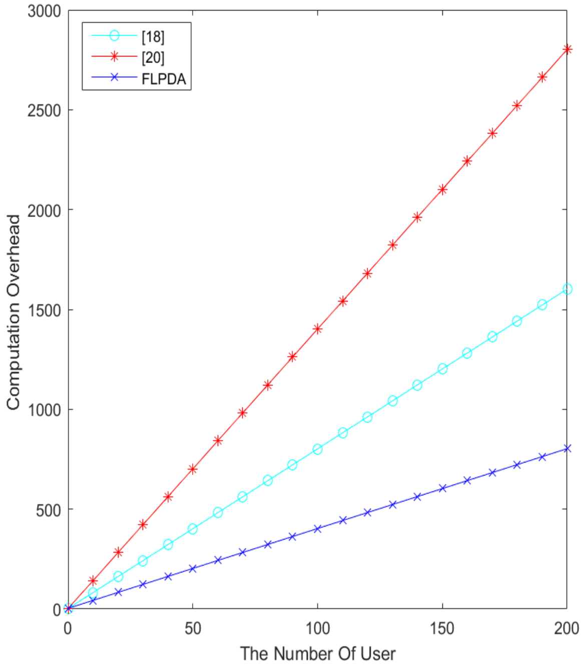

FIGURE 2. Comparison of computational overhead.

TABLE 4. Communication cost comparison.

Round	[18]	[20]	FLPDA
0	2M	2M	M
1	(4N-1) M	4NM	(N+1) M
2	NM	6NM	(N+1) M
3	M	6NM	(N+1) M
4	NM	M	M

VII. PERFORMANCE EVALUATION

A. COMPUTATION COMPLEXITY

To facilitate the comparison of FLPDA scheme with schemes [18] and [20], the execution time of each algorithm is listed in Table 3.

According to Table 3, it can be found that FLPDA scheme is more efficient than schemes [18] and [20]. In FLPDA scheme, due to batch signature verification, the signature verification is only 1/N of schemes [18] and [20]. Since scheme [18] or [20] generates N key pairs, the computational cost of key generation in FLPDA scheme is half that of scheme [18] or [20]. The number of key agreements for FLPDA scheme is 0, and the number of key agreements for scheme [18] or [20] is 2N times.

As shown in Figure 2, the calculation cost of FLPDA scheme is lower than that of scheme [18] or [20], which improves the response speed and enhances the practicality.

B. COMMUNICATION OVERHEAD

The comparison of communication costs between FLPDA and schemes [18] and [20] is shown in Table 4.

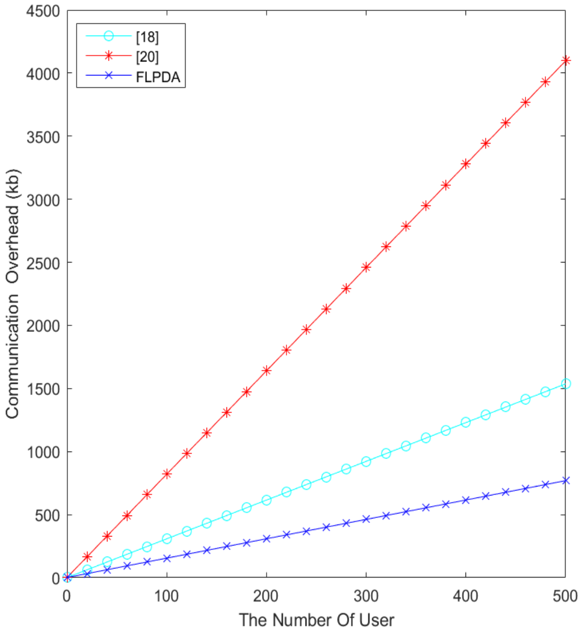

FIGURE 3. Comparison of communication overhead when M = 512 bits.

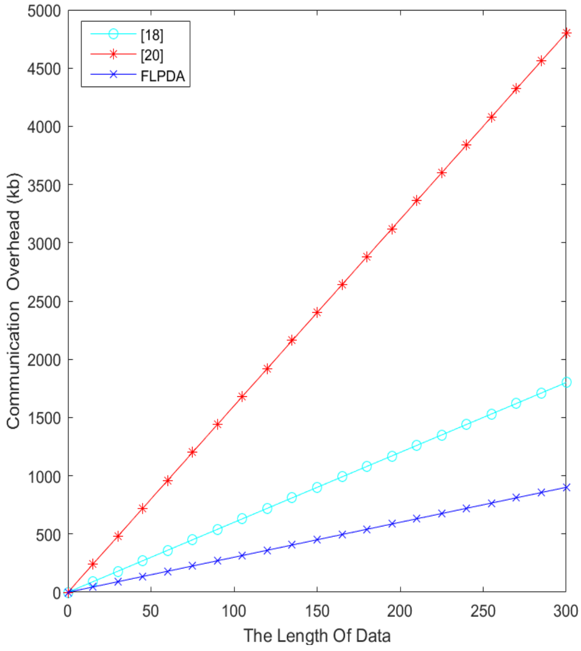

FIGURE 4. Comparison of communication overhead when N=1000.

TABLE 5. Storage cost comparison.

Round	[18]	LSHDA
0	3M	NM
1	6NM-3M	NM
2	3NM-2M	2NM
3	3NM-2M	4NM
4	3NM-2M	NM+M

In Table 4, FLPDA requires fewer communication costs than schemes [18] and [20], especially in Round 1. This means that if the FLPDA scheme is adopted, lower latency can be ensured, and practicality is improved.

N indicates the number of IIDs, and M bits indicate the data length. Figure 2 shows the communication costs comparison between FLPDA, [18] and [20] at M=512. Figure 4 shows the communication costs comparison between FLPDA, [18] and [20] when N=1000.

As shown in Figure 3 and Figure 4, FLPDA scheme has higher communication efficiency than schemes [18] and [20], especially the longer the data length, the more the number of IID, and the longer the data length, the more the communication cost will be saved.

C. STORAGE OVERHEAD

The storage costs of FLPDA scheme, scheme [18] and [20] are listed in Table 5. N represents the number of IIDs, and M bits represent the storage cost of each data to be sent. In Table 5, the calculated storage cost of each round for FLPDA scheme is compared with that for schemes [18] and [20].

In round 0, each IID needs to store an updated data request, so the storage cost of FLPDA is NM bits. In round 1, each IID needs to hold public key P_j, so the storage cost of FLPDA is NM bits. In round 2, each IID needs to keep $Ts \parallel E(y_j)\gamma_{y_j}$, so the storage cost of FLPDA is 2NM bits. In round 3, each IID needs to store $C_j \parallel P_j \parallel H_1(Ts \parallel E(y_j)\gamma_{y_j}) \parallel \sigma_j$, so the storage cost of FLPDA is 4NM bits. In round 4, each IID needs to store C_i, SN needs to store C, so the storage cost of FLPDA is (NM+M) bits.

As shown in Table 5, the total storage cost of FLPDA is (8N M+M) bits, and that of scheme [18] is (15NM-6M) bits. FLPDA scheme performs better than scheme [18] in terms of storage cost.

VIII. CONCLUSION

In this paper, a privacy-preserving data aggregation scheme based on Federated Learning for IIoT is proposed. Data aggregation is used to resist reverse analysis attacks and protect single user model changes in federated learning. The PBFT consensus algorithm is adopted to realize that it does not depend on any trusted entity. Combined with Paillier cryptosystem and secret sharing, the data security sharing is realized and the data island problem is solved. The analysis proves that the proposed scheme can resist various attacks and meet all design goals. Compared with existing schemes, our scheme has lower communication, computational, and storage costs. In the future, we will focus on improving the federated learning model to study multidimensional IoT data collection from the perspective of the physical layer.

REFERENCES

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[2] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[3] L. Cui, S. Yang, Z. Chen, Y. Pan, M. Xu, and K. Xu, "An efficient and compacted DAG-based blockchain protocol for industrial Internet of Things," *IEEE Trans. Ind. Informatics*, vol. 16, no. 6, pp. 4134–4145, Jun. 2019.

[4] Y. Guo, Z. Zhao, K. He, S. Lai, J. Xia, and L. Fan, "Efficient and flexible management for industrial Internet of Things: A federated learning approach," *Comput. Netw.*, vol. 192, Jun. 2021, Art. no. 108122.

[5] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, and Z. Yao, "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4231–4241, Jun. 2020.

[6] Q. Chen, S. Tang, Q. Yang, and S. Fu, "Cooper: Cooperative perception for connected autonomous vehicles based on 3D point clouds," in *Proc. IEEE 39th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jul. 2019, pp. 514–524.

[7] B. Zhao, X. Liu, W.-N. Chen, W. Liang, X. Zhang, and R. H. Deng, "PRICE: Privacy and reliability-aware real-time incentive system for crowdsensing," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17584–17595, Dec. 2021.

[8] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020.

[9] M. Nasr, R. Shokri, and A. Houmansadr, "Comprehensive privacy analysis of deep learning: Passive and active white-box inference attacks against centralized and federated learning," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2019, pp. 739–753.

[10] Y. Liu, G. Liu, C. Cheng, Z. Xia, and J. Shen, "A privacy-preserving health data aggregation scheme," *KSII Trans. Internet Inf. Syst. (TIIS)*, vol. 10, no. 8, pp. 3852–3864, 2016.

[11] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, and S. Kumari, "An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for Internet of Things (IoT) in mobile health (M-health) system," *J. Med. Syst.*, vol. 45, no. 1, pp. 1–14, Jan. 2021.

[12] H. Fan, Y. Liu, and Z. Zeng, "Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain," *Sensors*, vol. 20, no. 18, p. 5282, Sep. 2020.

[13] X. Ma, F. Zhang, X. Chen, and J. Shen, "Privacy preserving multi-party computation delegation for deep learning in cloud computing," *Inf. Sci.*, vol. 459, pp. 103–116, Aug. 2018.

[14] C. Liu, "An application of secure data aggregation for privacy-preserving machine learning on mobile devices," M.S. thesis, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2018.

[15] S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang, and Y. Zhou, "A hybrid approach to privacy-preserving federated learning," in *Proc. 12th ACM Workshop Artif. Intell. Secur.*, 2019, pp. 1–11.

[16] S. Sav, A. Pyrgelis, J. R. Troncoso-Pastoriza, D. Froelicher, J.-P. Bossuat, J. S. Sousa, and J.-P. Hubaux, "POSEIDON: Privacy-preserving federated neural network learning," 2020, *arXiv:2009.00349*.

[17] K. Bonawitz, V. Ivanov, B. Kreuter, A. Marcedone, H. B. Mcmahan, S. Patel, D. Ramage, A. Segal, and K. Seth, "Practical secure aggregation for privacy-preserving machine learning," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1175–1191.

[18] J. Song, W. Wang, T. R. Gadekallu, J. Cao, and Y. Liu, "EPPDA: An efficient privacy-preserving data aggregation federated learning scheme," *IEEE Trans. Netw. Sci. Eng.*, early access, Feb. 25, 2022, doi: 10.1109/TNSE.2022.3153519.

[19] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1918–1929, Mar. 2022.

[20] Q. Kong, F. Yin, R. Lu, B. Li, X. Wang, S. Cui, and P. Zhang, "Privacy-preserving aggregation for federated learning-based navigation in vehicular fog," *IEEE Trans. Ind. Informat.*, vol. 17, no. 12, pp. 8453–8463, Dec. 2021.

[21] Z. Zhou, Y. Tian, J. Xiong, J. Ma, and C. Peng, "Blockchain-enabled secure and trusted federated data sharing in IIoT," *IEEE Trans. Ind. Informat.*, early access, Oct. 17, 2022, doi: 10.1109/TII.2022.3215192.

[22] T. U. Islam, R. Ghasemi, and N. Mohammed, "Privacy-preserving federated learning model for healthcare data," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2022, pp. 281–287.

[23] K. Pillutla, S. M. Kakade, and Z. Harchaoui, "Robust aggregation for federated learning," *IEEE Trans. Signal Process.*, vol. 70, pp. 1142–1154, 2022.

[24] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, "Concurrent practical Byzantine fault tolerance for integration of blockchain and supply chain," *ACM Trans. Internet Technol.*, vol. 21, no. 1, pp. 1–17, Feb. 2021.

[25] J. Misic, V. B. Misic, and X. Chang, "Design of proof-of-stake PBFT algorithm for IoT environments," *IEEE Trans. Veh. Technol.*, early access, Oct. 10, 2022, doi: 10.1109/TVT.2022.3213226.

[26] Z. Guan, G. Si, X. Du, P. Liu, Z. Zhang, and Z. Zhou, "Protecting user privacy based on secret sharing with fault tolerance for big data in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

HONGBIN FAN received the B.S. degree in computer science and technology from Hengyang Normal University, Hengyang, China, in 2006, and the M.S. degree in computer application from Guangxi Normal University, Guilin, China, in 2009. He is currently pursuing the Ph.D. degree with the Army Engineering University of PLA, China. He was a Visiting Scholar at Hunan University, Changsha, China, from 2019 to 2020. He is currently a University Lecturer with the College of Computer and Artificial Intelligence, Xiangnan University, Chenzhou, China. His research interests include information security, federal learning, and blockchain technology.

CHANGBING HUANG received the B.S. degree in communication engineering from Hunan City University, Yiyang, China, in 2009, and the M.S. degree in communication engineering from the Guilin University of Electronic Technology, Guilin, China, in 2012. He is currently an Associate Professor with the Affiliated Hospital (Clinical College), Xiangnan University. His research interests include data privacy and information processing.

YINING LIU (Member, IEEE) received the B.S. degree in applied mathematics from Information Engineering University, Zhengzhou, China, in 1995, the M.S. degree in computer software and theory from the Huazhong University of Science and Technology, Wuhan, China, in 2003, and the Ph.D. degree in mathematics from Hubei University, Wuhan, in 2007. He is currently a Professor and a Doctoral Supervisor with the Guilin University of Electronic Technology, Guilin, China. His research interests include data privacy, image security, and machine learning.