Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 2381365, 13 pages
https://doi.org/10.1155/2022/2381365

*Research Article*

# A Blockchain-Based Privacy-Preserving Publish-Subscribe Model in IoT Multidomain Data Sharing

**Zhendong Liu,[1] Liang Meng,[1] Qingyuan Zhao,[1] Fei Li,[1] Manrui Song,[1] Dongxu Dai,[1] Xiujuan Yang,[1] Song Guan,[1] Yue Wang,[1] and Hongliang Tian[2]**

[1] *State Grid Benxi Electric Power Supply Company, Benxi 117000, China*
[2] *Jilin Northeast Electric Power University Science and Technology Development Co., Ltd., Jilin 132000, China*

Correspondence should be addressed to Hongliang Tian; hltian@foxmail.com

Received 24 June 2022; Accepted 18 September 2022; Published 14 October 2022

Academic Editor: Yin Zhang

With the dramatically increasing deployment of intelligent devices, the Internet of Things (IoT) has attracted more attention and developed rapidly. It effectively collects and shares data from the surrounding environment to achieve better IoT services. For data sharing, the publish-subscribe (PS) paradigm provides a loosely coupled and scalable communication model. However, due to the loosely coupled nature, it is vulnerable to many attacks, resulting in some security threats to the IoT system, but it cannot provide the basic security mechanisms such as authentication and confidentiality to ensure the data security. Thus, in order to protect the system security and users' privacy, this paper presents a secure blockchain-based privacy-preserving access control scheme for the PS system, which adopt the fully homomorphic encryption (FHE) to ensure the confidentiality of the publishing events and leverage the ledger to store the large volume of data events and access crossdomain information. Finally, we analyze the correctness and security of our scheme; moreover, we deploy our proposed prototype system on two computers and evaluate its performance. The experimental results show that our PS system can efficiently achieve the equilibrium between the system cost and the security requirement.

## 1. Introduction

With the rapid development of Internet of Things (IoT) in recent years, IoT devices deployed in application scenarios such as smart grid, smart city and smart home have increased sharply [1–3]. It was estimated that there will be over 24.9 billion IoT devices connected to the Internet by 2025 [4]. These interconnected mass terminal devices store and forward data to better realize system functions. As an attractive communication paradigm, publish-subscribe (PS) system can be used to build distributed data sharing across the Internet by separating the sender from the receiver. However, due to the loose coupling between publishers and subscribers, it is a challenge to provide security mechanisms such as authentication and confidentiality among each domain of the IoT [5]. Thus, we need to find out a method to ensure the data is only delivered to eligible subscribers who are interested and protect the confidentiality of the published events and the privacy of sensitive information in the process [6, 7].

Access control technology can protect the confidentiality, integrity, and availability of PS service and user data in the traditional IoT PS system. However, the traditional access control schemes cannot be used directly to provide fine-grained and scalable requirements for publish-subscribe systems [8]. The original publish-subscribe model relies on a trusted third-party broker such as MQTT [9], LooCI [10], and NesC [11], where data from all devices flows to subscribers through a central broker. Such a centralized architecture makes the PS model have the following disadvantages:

(i) The centralized architecture is vulnerable to a single point of failure. Since the broker is a centralized server, which coordinates the communication between the publishers and subscribers, if the server fails or is attacked by a malicious adversary, it may cause a large amount of sensitive information be compromised, thus threatening the privacy of the users and even making the whole system down

(ii) The semitrusted broker may be immoral, and it may lead to unauthorized access, abuse, and tampering with data

(iii) Since centralized servers rely on computationally greedy encryption algorithms, this is not suitable for computing resources-constrained IoT devices

Therefore, a novel decentralized PS model needs to be designed to address these issues. Due to the advantages of decentralization, anonymity and nontampering of records of blockchain [12, 13], it can provide reliable subscription record storage, subscription content forwarding, and subscription information verification for the PS system. The application of blockchain in the PS system has the following benefits:

(i) Decentralization: the published encrypted data and the subscription records are stored in blocks in the distributed ledger, and the consistency of network records is maintained through the consensus mechanism. Due to the decentralized nature of blockchain, it can increase the fault tolerance and antiaggression of the system, thus avoiding the impact of a single point of failure

(ii) Anonymity: all subscription contents are stored in the blockchain in an encrypted way, and the subscriber can access the data through its public key address. However, malicious users can only link to the public key address through hash pointer but do not know the real identity of the users

(iii) Nontampering: the subscription information is added to the blockchain after consensus verification, and then it will be recorded by all nodes together and related to each other through cryptography; so, tampering the data is very difficult and expensive

In order to solve the mentioned challenges in the PS system, this paper designs a novel blockchain-based PS model and proposes an access control mechanism based on the fully homomorphic encryption (FHE) algorithm [14] to protect the privacy of data sharing among multiple domains in the IoT. The proposed model mainly includes four entities: publishers, subscribers, broker based on private blockchain, and consortium blockchain, where publisher is responsible for publishing specific encrypted data, and subscriber receives related content by subscribing to the interested topics. Each broker based on private blockchain is composed of multiple distributed and decentralized gateway devices, and it only serves a subset of IoT devices to match user needs, delivers subscription content, and stores the subscription records, whereas the consortium blockchain connects private blockchain to facilitate crossdomain data sharing.

It is noteworthy that with the dramatically increasing of mobile services and applications, the broker needs to be equipped with more computing and storage capacity, but IoT devices are usually resource constrained, and they cannot bear the resource consumption caused by complex verification calculation of blockchain; so, we mitigate this problem by using edge computing. Edge computing utilizes nearby edge servers to bring real-time computations and communications [13, 15, 16]. As one way to process data at the network edge, it greatly expands the capacity and feasibility of terminal devices. In our model, we make full use of the private blockchain that has been formed through the gateway in [17], and then use the edge servers to create the consortium blockchain and perform FHE. By this way, it can provide publishers and subscribers with effective privacy protection. Our contributions are as follows:

(i) We propose a blockchain-based PS model for data sharing among multiple domains of IoT. This model eliminates the disadvantages of traditional PS model based on centralized broker and can make full use of consortium blockchain to carry out cross-domain subscription services in the large-scale IoT

(ii) We combine edge computing to provide computing power for data validation and all cryptographic computations and make it possible to deploy blockchain in the resource-constrained IoT. In addition, the cryptographic accumulator is used to quickly verify whether the subscription information on the one private blockchain is valid or not, which reduces the cost and latency of cross-domain data sharing

(iii) We use FHE with IND-CPA security to realize the attribute-based access control mechanism, so that the edge servers can perform arbitrary calculation of ciphertext without decryption, in this way, while ensuring the confidentiality and privacy of the subscription information and realizing the fine-grained access control of user data

The rest of this paper is organized as follows. Section 2 introduces some related work and briefly analyzes the pros and cons of various solutions. Section 3 reviews the preliminaries used in this paper. In Section 4, we present a blockchain-based privacy-preserving PS model. Section 5 analyses the performance and security of our scheme by deploying it on two computers. Finally, we summarize the paper with a further research discussion.

## 2. Preliminaries

In this section, we review some of the relevant theoretical basis of this study and briefly introduce and analyze the related background technologies, which mainly include the concepts of publish-subscribe system, attribute-based authorization, blockchain, fully homomorphic encryption, and edge computing.

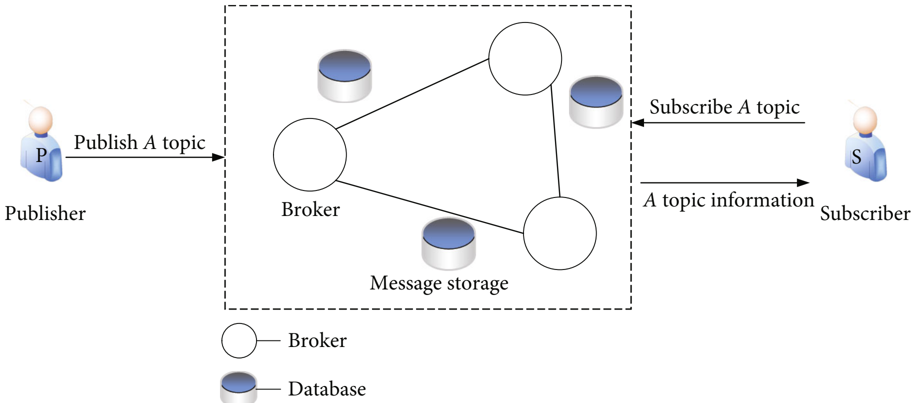

Figure 1: Publish-subscribe system architecture.

*2.1. Publish-Subscribe System.* Publish-subscribe system can be seen as a way of data-centric message distribution [18]. During the distribution of a message, the publisher can publish the message without specifying the identity of the user, and the subscriber also does not need to know the identity of the data owner to use message. In such a middleware solution, a message is represented as an event that can be detected in the application. As is shown in Figure 1, the PS model relies on three elements: publisher, subscriber, and the broker.

In the model, a publisher is an actor who generates any content and publishes it to the specified topic; subscriber is a user of events who subscribes the interested topics, and subscriber gets the published event when a publisher creates a publication for its subscription request. The broker is responsible for receiving the published events and notifying subscribers of the interested topics.

*2.2. Attribute-Based Authorization [19].* An attribute $A$ is defined as $A = (\mathrm{st}, \mathrm{value})$, meaning that the attribute st have value. A user has one attribute $A$ that can be represented by conjunctive formula $A_1 \Lambda A_2 \Lambda \cdots \Lambda A_t$. For a given system event topic tp, authorization policy restricts access to event data with a tp topic by using a user's specific attribute value.

*Definition 1.* The expression for an authorization policy is $\Lambda_{\mathrm{tp}} = (A_{11} \Lambda A_{12} \Lambda \cdots \Lambda A_{1t}) \mathrm{V} \cdots \mathrm{V} (A_{s1} \Lambda A_{s2} \Lambda \cdots \Lambda A_{st})$, which means that when a subscriber has at least a set of attributes from attribute concatenation $A_{11} \Lambda A_{12} \Lambda \cdots \Lambda A_{1t}$ to $A_{s1} \Lambda A_{s2} \Lambda \cdots \Lambda A_{st}$, the subscriber can access the data with topic tp.

For a subscriber whose attribute expression is $\omega = (A_{11}' \Lambda A_{12}' \Lambda \cdots \Lambda A_{1t}') \mathrm{V} \cdots \mathrm{V} (A_{h1}' \Lambda A_{h2}' \Lambda \cdots \Lambda A_{ht}')$, he/she has $h$ group connection attributes. As long as one of the $h$ group conjunctive attributes appears in $\Lambda_{\mathrm{tp}}$, then $\omega$ is defined to satisfy $\Lambda_{st}$.

*2.3. Blockchain and Edge Computing.* Since Nakamoto [12] published the Bitcoin white paper in 2008, the blockchain, as the underlying technology of Bitcoin, has quickly attracted a lot of attention due to its characteristics such as decentralization, no tampering, public verification and anonymity. The blockchain works as a distributed database that records all transactions that have occurred in the peer-to-peer (P2P) network. As is shown in Figure 2, the blockchain is a series of blocks connected one by one by hash. Blocks are added to the longest main blockchain by consistency protocol among most nodes in the network. Each block contains two parts: block header and block body, where all transactions involved in the block body, and the block header consists of the link pointers of the previous block header, a Merkle root of all transactions and a timestamp. Hyperledger Fabric [13, 20, 21] is a consortium blockchain based on distributed ledger. Unlike public or private blockchain, it executes the verification of transactions by a set of preselected nodes in the consortium blockchain, and the nodes can change dynamically; so, the consortium blockchain is more suitable for the scenario that supports node scalability.

Due to the limited computing capacity and available energy consumption of IoT terminal device, it has become the key bottleneck restricting the application of blockchain in IoT, but edge computing can help mitigate this problem. Edge computing transfers data processing from the remote cloud center to the edge of the network, and the computation and data storage can be dispersed to the edge of the Internet near the endpoint of things, sensors, and users. It brings real-time computation and communication by leveraging nearby edge servers.

*2.4. Fully Homomorphic Encryption [14].* Let $q$ be prime, $\mathbb{Z}_q$ be the integer field of modulo $q$, and $n$ be an integer. For the given plaintext $v \in \mathbb{Z}_q$ and the key $K$ generated by the parameters $q$ and $n$, there are encryption function $\mathrm{Enc}(K, v) = (c_1, c_2, \cdots, c_n)$ and decryption function $\mathrm{Dec}(K, (c_1, c_2, \cdots, c_n)) = v$, where ciphertext $(c_1, c_2, \cdots, c_n)$ is an $n$ -dimensional vector. Public key PK generated by key $K$ can be used to encrypt $v$, and then

$$\begin{aligned} \mathrm{Enc}(\mathrm{PK}, v) &= (c_1, c_2, \cdots, c_n), \\ \mathrm{Dec}(K, (c_1, c_2, \cdots, c_n)) &= v. \end{aligned} \tag{1}$$

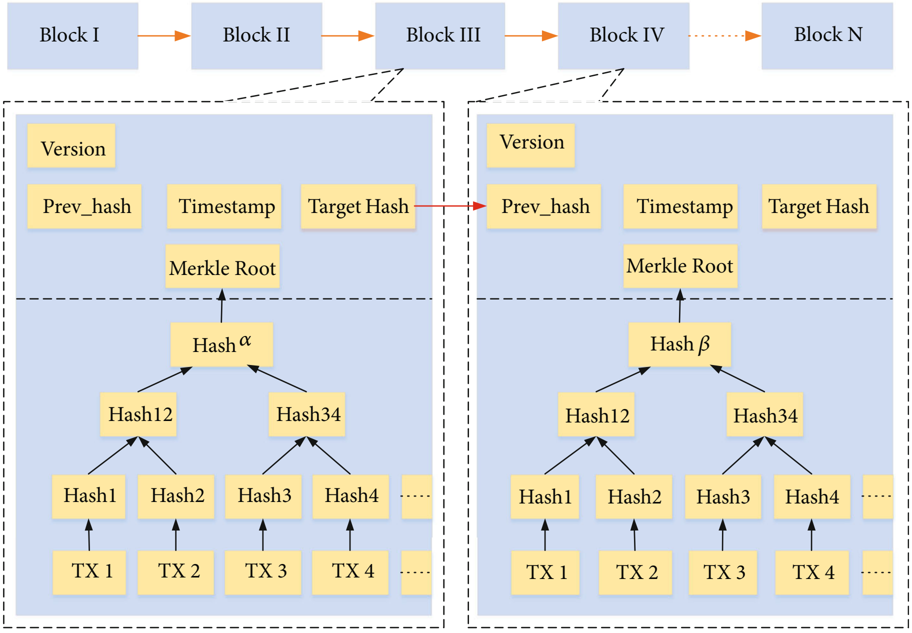

Figure 2: Blockchain structure.

Let $C = (c_1, c_2, \cdots c_n)$ and $C' = (c_1{}', c_2{}', \cdots, c_n{}')$. When $\mathrm{Dec}(K, C) = v$ and $\mathrm{Dec}(K, C') = v'$ exist in the decryption function, the FHE algorithm satisfies the following additional homomorphism properties:

$$\begin{gathered}\mathrm{Dec}\left(K, C \oplus C'\right) = v + v' (\mathrm{mod}\ q),\\ \mathrm{Dec}(K, d \square C) = d * v (\mathrm{mod}\ q),\end{gathered} \tag{2}$$

where $\oplus$ is vector addition, and $\square$ is scalar multiplication of vectors.

The homomorphic operation of multiplication also requires the public evaluation key $\mathrm{PEK}_{ij} (1 \leq i \leq n, 1 \leq j \leq n)$, which is generated by $K$. For $v * v'$ obtained from ciphertext $C$ and $C'$, it can be expressed as

$$\left(\left(c_1 * c_1{}'\right) \square \mathrm{PEK}_{11}\right) \oplus \cdots \oplus \left(\left(c_i * c_j{}'\right) \square \mathrm{PEK}_{ij}\right) \oplus \cdots \oplus \left(\left(c_n * c_n{}'\right) \square \mathrm{PEK}_{nn}\right). \tag{3}$$

For a given publisher's secret key $\mathrm{sk}_p$ and subscriber's public key $\mathrm{pk}_s$, the ciphertext encrypted with $\mathrm{sk}_p$ can be converted to the ciphertext encrypted with subscriber's secret key $\mathrm{sk}_s$. The key exchange process is as follows:

Let $\mathrm{KeySwitch}(\mathrm{pk}_s, \mathrm{sk}_p)$ be the generating function of exchange key KS, and then $\mathrm{KS} = \{\mathrm{KS}_1, \mathrm{KS}_2, \cdots, \mathrm{KS}_n\}$, where any $\mathrm{KS}_i$ is an $n$-dimensional vector. Suppose there is $\mathrm{Decrypt}(\mathrm{sk}_p, (c_1, c_2, \cdots, c_n)) = v$, then the reencryption of ciphertext $C$ with exchange key KS can be expressed as $\mathrm{ReEnc}(\mathrm{KS}, C) = (c_1 \square \mathrm{KS}_1) \oplus (c_2 \square \mathrm{KS}_2) \oplus \cdots \oplus (c_n \square \mathrm{KS}_n),$, let $C' = \mathrm{ReEnc}(\mathrm{KS}, C)$, and then $\mathrm{Dec}(sk_s, C') = v$.

## 3. Related Work

In recent years, most of the research on PS system has focused on effective event routing, event filtering, and composite event detection, and little has been done to address privacy issues. Here, we briefly summarize some relevant work in recent years and find that it can be divided into two categories: (1) PS system based on traditional broker server and (2) PS system based on P2P (peer-to-peer) network. This section mainly analyzes the current research status of privacy-preserving PS system.

*3.1. Based on Traditional Broker Servers.* Duan et al. [22] proposed a comprehensive access control framework CACF to guarantee the data confidentiality and service privacy of the publish-subscribe model in different domains. It uses fully homomorphic encryption to encrypt data and bidirectional privacy-preserving policy to match access policies and subscription policy. We can see from the performance analysis result that the CACF scheme can provide confidentiality and privacy-preserving with acceptable latency, but the centralized message-oriented Java Message Service (JMS) broker can cause a single point of failure.

AKPS [23] is a privacy-preserving attribute-keyword-based data publish-subscribe scheme. This scheme uses attribute-based encryption with decryption outsourcing to encrypt the published data. While realizing the publisher's own control of data access, it transfers the main decryption overhead from subscribers to the cloud server. And subscribers who search by keyword can choose to receive the data according to their own interests. However, the publisher has only one identity; that is, it cannot receive the information as a subscriber.

In [24], Wang et al. proposed a privacy protection scheme for a content-based publish/subscribe system with

Table 1: The comparison with other schemes.

| Scheme | Confidentiality | Decentralized | Privacy | Fine-grained access | Against collusion attack | Against spoofing attacks |
|---|---|---|---|---|---|---|
| Duan et al. [22] | ✓ | — | ✓ | ✓ | ✓ | ✓ |
| Yang et al. [23] | ✓ | — | ✓ | ✓ | — | — |
| Wang et al. [24] | ✓ | — | ✓ | — | ✓ | — |
| Diro et al. and Diro et al. [25, 26] | ✓ | — | ✓ | — | — | — |
| Borcea et al. [27] | ✓ | — | ✓ | — | — | — |
| Zhao et al. [28] | ✓ | ✓ | ✓ | — | ✓ | ✓ |
| Lv et al. [29] | ✓ | ✓ | ✓ | — | — | ✓ |
| Tariq et al. [30] | ✓ | ✓ | — | — | — | — |
| Our scheme | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

differential privacy in a fog computing environment. It used the $U$-Apriori algorithm to extract the collection of the first $K$ frequent items from uncertain data sets and then applied the exponential and Laplace mechanism to ensure differential privacy. Brokers mine the first $K$ item sets to eventually match the appropriate publishers and subscribers. This method reduces the cost of user computation and storage, but the complex attribute matching method increases the delay of matching time and increases with the number of users.

In order to provide basic security mechanisms for fog computing-based publish-subscribe system in IoT, Diro et al. [25] proposed a secure lightweight publish-subscribe protocol based on elliptic curve cryptography (ECC). It reduces the overhead of computations, storage, and communications in traditional security protocols such as SSL/TSL. In [26], Diro et al. proposed a resource efficient end-to-end security scheme by offloading computations and storage of security parameters to fog nodes in the vicinity. In addition, a symmetric-key payload encryption has been used to minimize the overhead of message communication in the resource-contested IoT environment.

Borcea et al. [27] introduced PICADOR, a topic-based publish-subscribe system designed using proxy reencryption. This system provides end-to-end encrypted information distribution service, and it ensures the information confidentiality between publishers and subscribers without sharing encryption and decryption keys. The system not only reduces the communication cost but also reduces the vulnerability of internal attack. However, reencryption also brings a heavy computing burden to proxy server.

*3.2. Based on P2P Network.* Zhao et al. [28] built a fair and secure publish-subscribe system (SPS) based on blockchain. In SPS, in order to realize fair data exchange, publishers publish a topic on the blockchain, and subscribers subscribe the interested topic by deposit. At the same time, the publisher and subscriber use hybrid encryption to ensure data confidentiality and take advantage of the pseudoanonymity of bitcoin system to ensure the identity privacy of both parties. However, because this scheme cannot provide fine-grained access control, it cannot provide users with more accurate and efficient services according to their own features.

In [29], Lv et al. propose a privacy-preserving publish/subscribe model by using the blockchain technique, which ensures the system confidentiality by employing public key encryption with equality test (PKEwET), and they solved the single point of failure and the anonymity of the participants by using the Ethereum.

Tariq et al. [30] proposed a new approach to provide authentication and confidentiality in broker-less content-based publish/subscribe system. Credentials are assigned to publishers and subscribers by adapting the pairing-based cryptography mechanisms. Because the private keys and ciphertext assigned to publishers and subscribers are marked with credentials, a particular subscriber can decrypt an event only if the credentials associated with the event match the private key. However, Tariq et al. do not consider the anonymity of subscriber.

In [31], the authors contributed Trinity, a novel distributed publish-subscribe broker with blockchain-based immutability. It distributes the published data to all brokers in the network and stores the distributed data in an immutable ledger by using the blockchain technology. In this way, it can guarantee persistence, ordering, and immutability across trust boundaries, but the Trinity framework increases the end-to-end delay while consuming bandwidth and computation resources.

Gao et al. [32] proposed a new trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain, named TrustAccess, to achieve trustworthy access. To address the privacy issues of access policy and user attribute in the TrustAccess, an optimized hidden policy CP-ABE named OHP-CP-ABE to ensure policy privacy while satisfying the large universe access requirement. In addition, the authors use the multiplicative homomorphic ElGamal cryptosystem to ensure the attribute privacy during authorization validation.

## 4. BPAC System Model

In this section, we mainly explain how the proposed blockchain-based IoT publish-subscribe system works. For convenience, some notations will appear in our BPAC scheme as shown in Table 1.

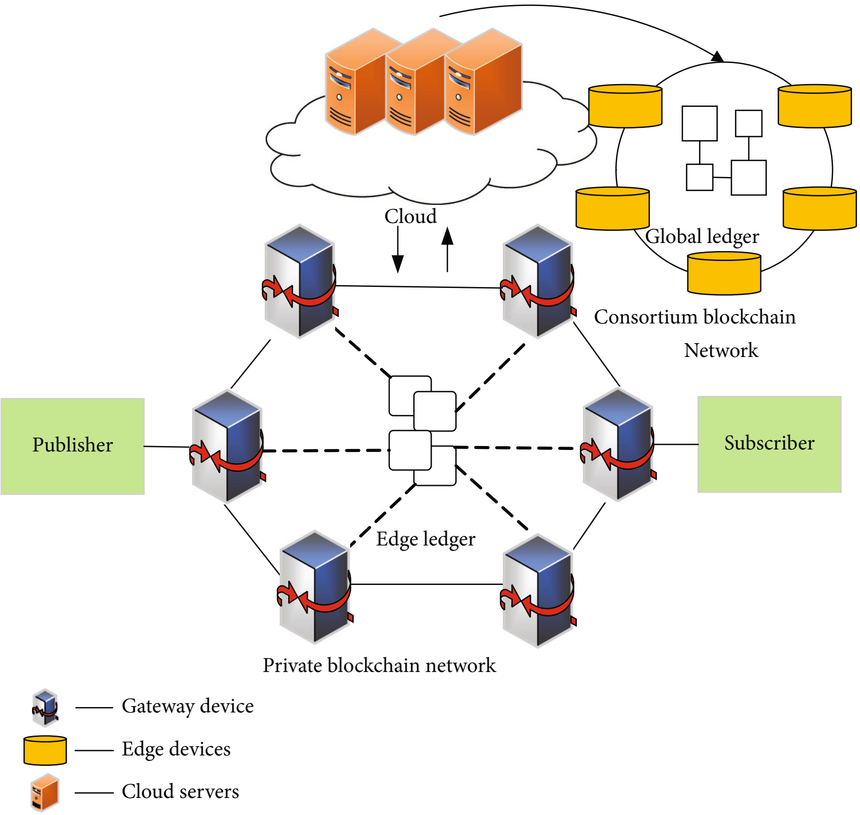

Figure 3: Security access control system model.

*4.1. Security Model.* In our work, we assume the certificate authority (CA) that creates the public/private keys for the publisher or subscriber and assigns public parameters to the system is honest; that is, the CA follows the rules to perform computations. And the publisher who can correctly and truly publish the encrypted data is legal. All published events are stored in the global ledger maintained by the edge devices, and all data validation and publish-subscribe services processing are performed by the edge devices to reduce the workload of an IoT device. It is worth emphasizing that the storage and protection of the published events are only performed by blockchain, without intervention of any other entity. Therefore, the security of our scheme is mainly guaranteed by blockchain. In our scheme, publishers and subscribers within the domain directly interact with each other through private blockchain, and the crossdomain users connect private blockchain through consortium blockchain for temporary crossdomain information interaction. In the actual collaborative IoT services, there may have a many-to-many relationship among multiple publishers and subscribers. Here, we just take one publisher and one subscriber to discuss the access control procedure in our framework. The system model is shown in Figure 3.

*4.2. Blockchain-Based Security Publish-Subscribe System.* We propose a secure PS scheme which is based on FHE [14]. Assume that a publisher $P$ contains a key pair $(\mathrm{PK}_p, \mathrm{SK}_p)$, and a subscriber $S$ contains a key pair $(\mathrm{PK}_s, \mathrm{SK}_s)$. The specific dynamic data flow is shown in Figure 4. The access control procedure mainly contains the following phases: Setup, Publish, Subscribe, Match, and Receive.

*4.2.1. Setup.* The setup algorithm takes the security parameter $\lambda$, a number of levels $L$, and $b \in \{0, 1\}$ as input parameters to generate the system parameter $\mathrm{Params} = (q, d, n, N, \chi)$. This algorithm is run by CA, and only CA knows the value of Params, where let $\mu = \mu(\lambda, L, b)$, whose modulus is prime $q$, and $d = d(\lambda, \mu, b)$, $n = n(\lambda, \mu, b)$, $N = N(\lambda, \mu, b)$, and $\chi = \chi(\lambda, \mu, b)$. Finally, the key pair PK and SK are generated as follows:

$$\begin{aligned} \mathrm{SecretKeyGen}(\mathrm{params}) &\longrightarrow \mathrm{SK}, \\ \mathrm{PublicKeyGen}(\mathrm{params}) &\longrightarrow \mathrm{PK}, \end{aligned} \tag{4}$$

where the key pair of publisher and subscriber is, respectively, $(\mathrm{PK}_p, \mathrm{SK}_p)$ and $(\mathrm{PK}_S, \mathrm{SK}_S)$.

*4.2.2. Publish.* The publisher randomly selects random number $r_{\mathrm{pp}}, r_{\mathrm{up}}, r_{\mathrm{ac}}$ and hash function $h$ in advance, where $r_{\mathrm{pp}}$ is greater than the number of topics in the publishing event $e_{\mathrm{tp}}$, then generates $h_{\mathrm{up}} = h(\mathrm{A}_{i1} \| \mathrm{A}_{i2} \| \cdots \| \mathrm{A}_{\mathrm{im}} \| r_{\mathrm{up}})$, and encrypts event $e_{\mathrm{tp}}$ with topic tp and policy $\varLambda_{\mathrm{tp}} = (\mathrm{A}_{11} \varLambda \mathrm{A}_{12} \varLambda \cdots \varLambda \mathrm{A}_{1t}) \mathrm{V} (\mathrm{A}_{s1} \varLambda \mathrm{A}_{s2} \varLambda \cdots \mathrm{A}_{\mathrm{st}})$ as $C_{\mathrm{tp}}$ through edge servers. For each set of attribute conjunction formula $\mathrm{A}_{i1} \varLambda \mathrm{A}_{i2} \varLambda \cdots \varLambda \mathrm{A}_{im} (1 \leq i \leq n)$, the publisher generates $F_s$ through the attribute filter function $F(\mathrm{A}_{i1} \varLambda \cdots \varLambda \mathrm{A}_{im})$, uses the edge servers

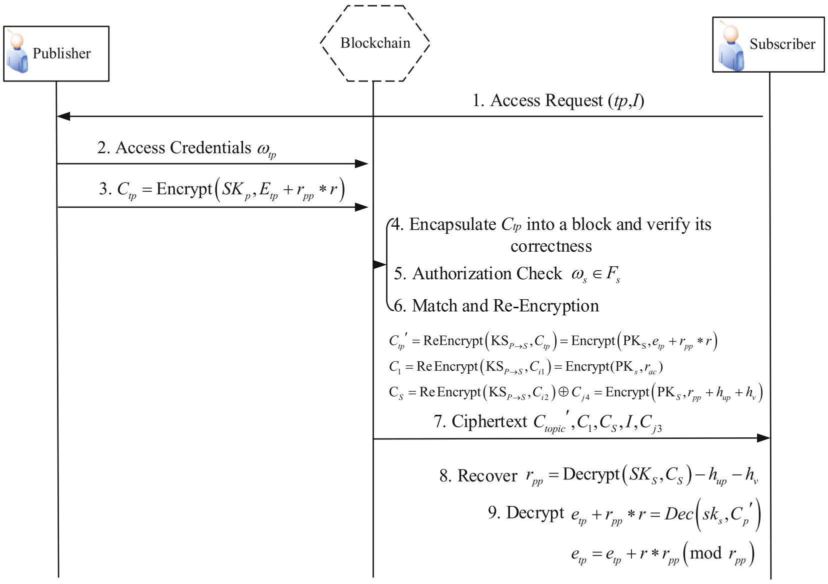
Publisher
Blockchain
Subscriber
1. Access Request (*tp*,*I*)
2. Access Credentials $\omega_{tp}$
3. $C_{tp} = \text{Encrypt}\left(SK_p, E_{tp} + r_{pp} * r\right)$
4. Encapsulate $C_{tp}$ into a block and verify its correctness
5. Authorization Check $\omega_s \in F_s$
6. Match and Re-Encryption
$C_{tp}' = \text{ReEncrypt}\left(\text{KS}_{P\to S}, C_{tp}\right) = \text{Encrypt}\left(\text{PK}_S, e_{tp} + r_{pp} * r\right)$
$C_1 = \text{Re}\,\text{Encrypt}\left(\text{KS}_{P\to S}, C_{i1}\right) = \text{Encrypt}(\text{PK}_s, r_{ac})$
$\text{C}_S = \text{Re}\,\text{Encrypt}\left(\text{KS}_{P\to S}, C_{i2}\right) \oplus C_{j4} = \text{Encrypt}\left(\text{PK}_S, r_{pp} + h_{up} + h_v\right)$
7. Ciphertext $C_{topic}', C_1, C_S, I, C_{j3}$
8. Recover $r_{pp} = \text{Decrypt}\left(SK_S, C_S\right) - h_{up} - h_v$
9. Decrypt $e_{tp} + r_{pp} * r = Dec\left(sk_s, C_p'\right)$
$e_{tp} = e_{tp} + r * r_{pp}\left(\text{mod } r_{pp}\right)$

FIGURE 4: Interactive time sequence in our scheme.

to convert it into access credentials:

$$\omega_{\text{topic}} = \begin{pmatrix} \text{KS}_{P\longrightarrow S}, \{(C_{11}, C_{12}, F_1), (C_{21}, C_{22}, F_2),\cdots,(C_{s1}, C_{s2}, F_s)\} \\ \{(C_{13}, C_{14}), (C_{23}, C_{24}),\cdots,(C_{h3}, C_{h4})\} \end{pmatrix}, \tag{5}$$

and finally publishes $F_s$ and $C_{tp}$ on a private blockchain. The encryption process for publishing events is as follows:

$$\begin{aligned} C_{i1} &= \text{Encrypt}\left(\text{SK}_P, r_{up}\right), \\ C_{i2} &= \text{Encrypt}\left(\text{SK}_P, h_{\text{up}} + r_{\text{pp}} - r_{\text{ac}}(h(A_{i1}) + h(A_{i2}) + \cdots + h(A_{im}))\right), \\ C_{j3} &= \text{Encrypt}(PK_S, r_S), \\ \text{C}_{j4} &= \text{Encrypt}\left(PK_S, h_v + r_{\text{ac}}\left(h\left(A_{j1}'\right) + h\left(A_{j2}'\right) + \cdots + h\left(A_{jm}'\right)\right)\right). \end{aligned} \tag{6}$$

When the private blockchain receives the encrypted event $C_{tp}$, the edge servers packaged it into a block and stored in the edge ledger after being authenticated by the whole network.

*4.2.3. Subscribe.* First, the subscriber *S* with property expression $\omega_s = (\text{A}_{11}'\Lambda\text{A}_{12}'\Lambda\cdots\Lambda\text{A}_{1t}')\text{V}\cdots\text{V}(\text{A}_{h1}'\Lambda\text{A}_{h2}'\Lambda\cdots\text{A}_{ht}')$ subscribes to an interested topic through edge ledger, and then subscriber encrypts its property index value *j* to $I = \text{Encrypt}(PK_s, j)$ and finally sends it to the private blockchain broker.

*4.2.4. Match and Key Switching.* When the publisher receives a subscription request from the subscriber, it first checks whether subscriber's attribute conjunction $\omega_s$ satisfies $\omega_s \in F_s$. If the condition is met, the subscriber is certified as a valid user, and his subscription request is allowed. Then, the publisher will reencrypt the ciphertext $C_{tp}, C_{i1}, C_{i2}$ through edge servers to $C_{tp}', C_1, C_s$. The conversion process is as follows:

$$\begin{aligned} C_{\text{tp}}' &= \text{ReEncrypt}\left(\text{KS}_{P\longrightarrow S}, C_{\text{tp}}\right) = \text{Encrypt}\left(\text{PK}_S, e_{\text{tp}} + r_{\text{pp}} * r\right), \\ C_1 &= \text{Re Encrypt}(\text{KS}_{P\longrightarrow S}, C_{i1}) = \text{Encrypt}(\text{PK}_s, r_{ac}), \\ \text{C}_S &= \text{Re Encrypt}(\text{KS}_{P\longrightarrow S}, C_{i2}) \oplus C_{j4} = \text{Encrypt}\left(\text{PK}_S, r_{\text{pp}} + h_{\text{up}} + h_v\right). \end{aligned} \tag{7}$$

Finally, the publisher authorizes the subscriber *S* to access $C_{tp}', C_1, C_s, I$ and $C_{j3}$ from the edge ledger.

If subscriber *S* fails to meet the requirement, the edge servers simply refuse the subscriber's access requests.

*4.2.5. Receive.* After subscriber *S* receives $C_{tp}', C_1, C_s, I$ and $C_{j3}$, it first decrypts *I* to obtain index *j*, thus obtaining the authorization attribute conjunction $\omega_j = A_{j1}'\Lambda A_{j2}'\Lambda\cdots\Lambda A_{jm}'$. Then it decrypts $C_{j3}$ and $C_1$ to get the random values $r_s$ and $r_{ac}$. Then, the subscriber uses hash function *h* to restore $r_{\text{pp}}$:

$$\begin{aligned} h_{\text{up}} &= h\left(\text{A}_{j1}'\|\text{A}_{j2}'\|\cdots\|\text{A}_{\text{jm}}'\|r_{\text{up}}\right), \\ h_v &= h\left(\text{A}_{j1}'\|\text{A}_{j2}'\|\cdots\|\text{A}_{\text{jm}}'\|r_S\right), \\ r_{\text{pp}} &= \text{Decrypt}(\text{SK}_S, C_S) - h_{\text{up}} - h_v. \end{aligned} \tag{8}$$

Finally, the subscriber decrypts the ciphertext $C_{\text{tp}}'$ and gets $e_{\text{tp}} + r_{\text{pp}} * r$, and the modular operation is then performed on $r_{\text{pp}}$ to recover the event $e_{\text{tp}}$.

*4.3. Efficient Crossdomain Access and Authentication.* For the crossdomain PS system, there is no direct connection among edge ledgers, and no copies of other ledgers are

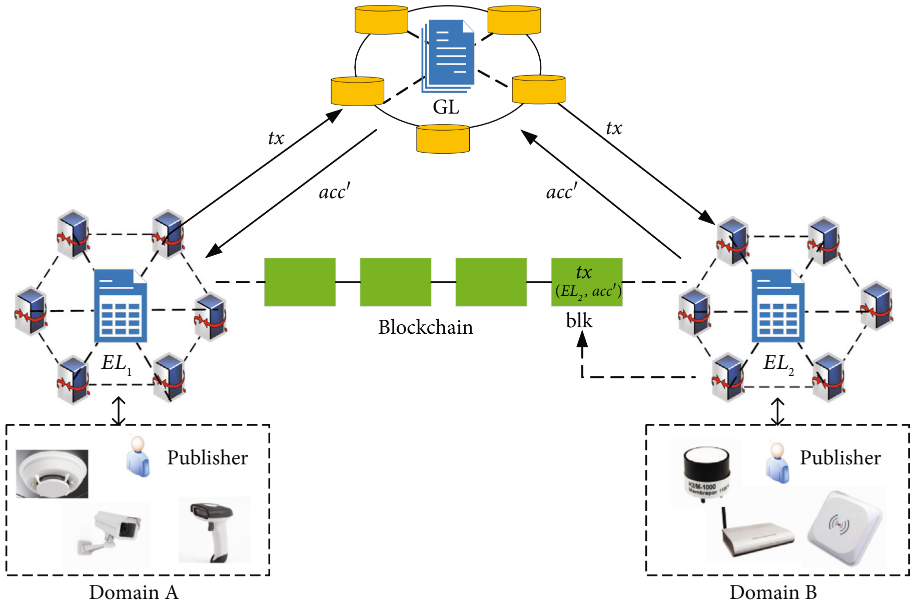

Figure 5: Crossdomain data verification.

kept. Therefore, after obtaining the authorization information, the subscriber needs to verify whether the authorization information block belonging to another edge ledger is valid.

Assume that $\mathrm{EL}_1$ and $\mathrm{EL}_2$ are two subscribers of edge ledger in different domains. $\mathrm{EL}_1$ needs to access the publishing events in $\mathrm{EL}_2$ through the global ledger GL and verifies its validity. The verification process after obtaining the authorization information block is shown in Figure 5.

(1) $\mathrm{EL}_2$ processes the new authorization information block tx

(i) $\mathrm{EL}_1$ initiates a verification request for information block tx to the global ledger GL. GL forwards it to $\mathrm{EL}_2$ and $\mathrm{EL}_2$ initializes the value acc of the accumulator after receiving the verification request

(ii) $\mathrm{EL}_2$ packs tx into a new block blk and updates the accumulator value to $\mathrm{acc}'$

(iii) All nodes $\mathrm{el}_{2j}$ in $\mathrm{EL}_2$ run the consensus protocol to add blk and update accumulator value $\mathrm{acc}'$ to the blockchain

(2) $\mathrm{EL}_2$ updates its status to GL

(i) $\mathrm{EL}_2$ only updates the accumulator value to GL after a certain number of new blocks are created

(ii) GL checks whether $\mathrm{EL}_2$ has achieved consensus on $\mathrm{acc}'$, if it passes the check, then the latest state of $(\mathrm{EL}_2, \mathrm{acc}')$ is included in the new block

(3) $\mathrm{EL}_1$ checks the validity of tx

(i) $\mathrm{EL}_1$ obtains the current accumulator value of $\mathrm{EL}_2$ from GL

(ii) $\mathrm{EL}_1$ requests $\mathrm{EL}_2$ to provide evidence that block blk contains the authorization information block tx

(iii) $\mathrm{EL}_2$ responses to $\mathrm{EL}_1$'s request and provides a proof that blk is included in the edge ledger $\mathrm{EL}_2$

$\mathrm{EL}_1$ verifies the evidence. After verification, it can utilize the information in tx.

## 5. Security and Performance Analysis

In this section, we first theoretically analyze the security of the proposed scheme and illustrate the correctness of our scheme, where our scheme only aims to resist collusion attack and spoofing attacks. Then, we implement the prototype system to evaluate its performance.

### 5.1. Security Analysis

*5.1.1. Confidentiality.* For our proposed publish-subscribe scheme, the security of data sharing is based on the security of blockchain and FHE algorithm. Among them, since the FHE is IND-CPA secure, that is to say, an adversary first gets a properly generated pk, then specifies message

$m_0, m_1 \in R_M$ ($R_M$ is a message ring), and finally gets $\mathrm{Enc}_{pk}(m_b)$ for a random number $b$; it cannot guess the value of $b$ with probability $>1/2+\varepsilon(\lambda)$, where $\varepsilon$ is a negligible function in the security parameter $\lambda$. In other words, for a given ciphertext, an adversary is not able to know any useful information about the corresponding plaintext; that is, it is secure against chosen-plaintext attack. And we adopted the FHE algorithm to set up a credible PS system for IoT, which can separate data processing rights and data ownership, so as to prevent data privacy leakage while using edge servers computing power. In addition, blockchain lies on the hardness of preventing sibyl attacks and DDoS attacks. In the large-scale IoT environments, with more IoT devices connected to the blockchain network, the more gateway nodes in the network increases, and the more security will be improved; so, it is difficult for an attacker to launch a DDoS attacks in the blockchain network. This is because if you want to launch 51% attacks in the blockchain network, you need a lot of computing power to control the nodes that are distributed everywhere, since an adversary is not powerful enough to take over the majority of the nodes. Therefore, the scheme can guarantee the confidentiality of the message.

*5.1.2. Resistance to Collusion Attack.* For two collusive subscribers $S_1$ and $S_2$, they cannot successfully pass the inspection of the property filter function $F$ in the edge servers, because neither of them has the authentication attribute authorized by the access control policy. Even if the edge servers are malicious and also participate in the collusion attack, consequently, make both pass the inspection and convert keys to generate $C_p{}''$, $C_1{}'$, $C_s{}'$, $I'$, $C_{j3}{}'$ and $C_p{}'''$, $C_1{}'$, $C_s{}''$, $I''$, $C_{j3}{}''$. However, $S_1$ and $S_2$ will only get the following ciphertext:

$$C_S{}' = \mathrm{Encrypt}\left(\begin{matrix} \mathrm{PK}_{S_1}, r_{\mathrm{pp}} + h_{\mathrm{up}}{}' + h_v{}' + \\ r_{ac} * \left(\begin{matrix} h\left(A_{k1}{}'\right) + h\left(A_{k2}{}'\right) + \cdots + h\left(A_{\mathrm{km}}{}'\right) - \\ h(A_{i1} - A_{i2} - \cdots A_{\mathrm{im}}) \end{matrix}\right) \end{matrix}\right),$$

$$C_S{}'' = \mathrm{Encrypt}\left(\begin{matrix} \mathrm{PK}_{S_2}, r_{\mathrm{pp}} + h_{\mathrm{up}}{}'' + h_v{}'' + \\ r_{\mathrm{ac}} * \left(\begin{matrix} h\left(A_{q1}{}'\right) + h\left(A_{q2}{}'\right) + \cdots + h\left(A_{\mathrm{qm}}{}'\right) - \\ h(A_{w1} - A_{w2} - \cdots - A_{\mathrm{wm}}) \end{matrix}\right) \end{matrix}\right). \tag{9}$$

But since $S_1$ and $S_2$ do not know the values of $r_{ac}$, $A_k$, $A_\omega$, so $S_1$ and $S_2$ cannot recover $r_{\mathrm{pp}}$ and the event $e_{\mathrm{tp}}$.

*5.1.3. Resistance to Spoofing Attacks.* In our scheme, an edge server is placed in the same local network as the IoT devices, aiming to help the IoT devices perform certain kinds of computations. If the edge server is fake, it may fake the access credentials to recover event $e$, but it does not have any private keys of the subscribers to decrypt ciphertexts. At the same time, if an edge device tries to forge encrypted data while performing cryptographic computations, it will be detected and excluded by other nodes in the consortium blockchain. In addition, the consortium blockchain composed of edge devices has a certain fault-tolerant. Even if there are false malicious nodes in the network, as long as the number does not exceed 1/3 of the total number of nodes, it can guarantee the normal and stable operation of the system. So, even if the edge devices are fake, as long as there are enough honest nodes in the network, our scheme is also available.

### 5.2. Correctness Analysis

**Theorem 2.** *For the access control policy $\Gamma_{topic} = (A_{11} \Lambda A_{12} \cdots \Lambda A_{1m}) V \cdots V(A_{n1} \Lambda A_{n2} \Lambda \cdots A_{nm})$ of an event $e$ with a topic tp, and an attribute conjunction $\gamma = (A_{11}{}' \Lambda A_{12}{}' \Lambda \cdots \Lambda A_{nm}{}')$ of a subscriber S, when $1 \le j \le m$ and $1 \le j \le k$, and $A_{i1} = A_{j1}{}', \cdots, A_{im} = A_{jm}{}'$, then S can access all events of topic tp.*

*Proof.* In our scheme, the edge servers generate $C_p{}'$, $C_1$, $C_s$, $I$ and $C_{j3}$ for subscriber $S$, and $S$ finally gets event $e$ by decrypting it. When $e_{tp} + r_{pp} * r = e_{tp} (\mathrm{mod}\ r_{pp})$, if $r_{pp} > e_{tp}$, then Theorem 2 is satisfied; so, our scheme satisfies correctness. □

We also compare our scheme with other related work from the aspects of confidentiality, data privacy, decentralization, fine-grained access, collusion resistance, and ant-spoofing attack in Table 1, and the specific comparison results are described in Table 1.

As is shown in Table 1, all solutions are realized data event confidentiality; however, the proposed PS systems adopt centralized architecture in literature [22–27], in which all data are published to the subscriber by central broker, such a centralized architecture is vulnerable to the effects of a single point of failure, and the broker who is not fully trusted may leak or tamper with data, thus causing some insecure factors and posing a threat to the stable operation of the system. On the other hand, the data owner should have the right to determine who can use the data it provides, while in [24–30], there did not reflect the control of publishers over the authorization granularity for different information and subscribers. And subscribing services can be dishonest in practice, and the subscribers may attempt to access unauthorized events by colluding with each other, but most of the other work did not consider this problem. On the contrary, our scheme can better solve the above problems.

*5.3. Performance Analysis.* In order to verify the availability and performance of our proposed BPAC mechanism, we deployed our prototype system on two computers: the publisher/subscriber and blockchain broker both ran on the configured with 8.0G of RAM, AMD 2.3GHz CPUs, and Windows10_64 operating system, which the private blockchain is built on Ethereum. Furthermore, we use the Hyperledger Fabric deployed on the IBM Cloud platform for the consortium blockchain. Here, we use system throughput and two types of time delay as the main performance

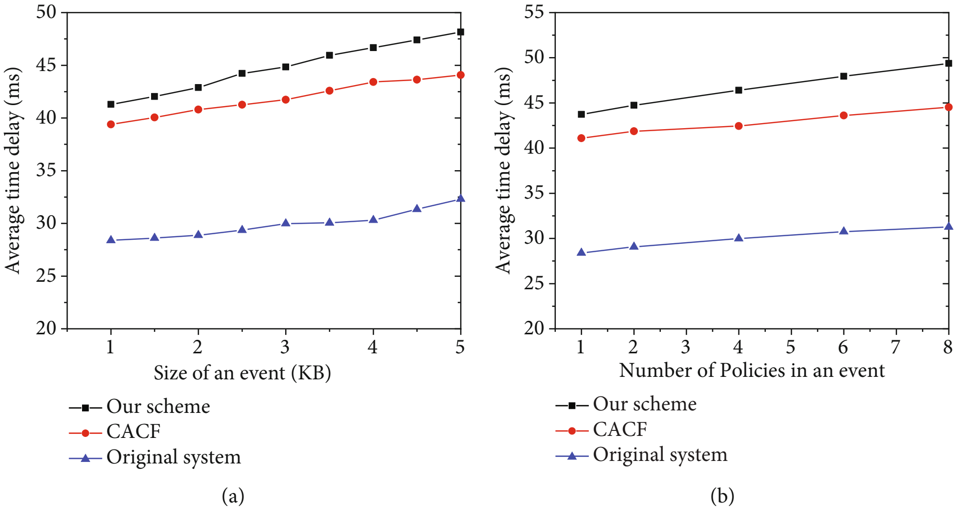

Figure 6: This is system delay and throughput with different event sizes: (a) latency with different sizes of one event (KB) and (b) throughput for different event sizes in KB.

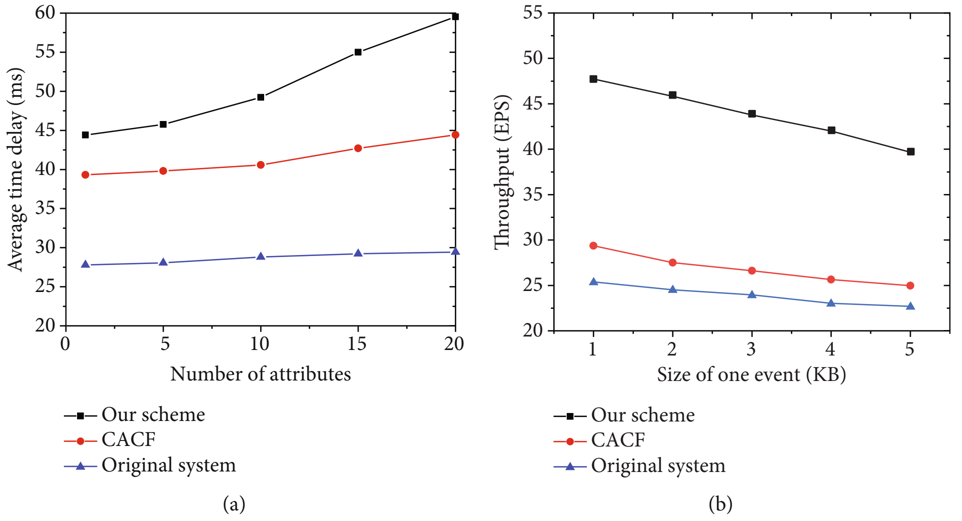

Figure 7: This is system delay with different numbers of attributes and policies: (a) latency with different numbers of attributes on one subscriber and (b) latency with different numbers of policies in one event.

evaluation criteria: (1) PS prototype system without using our proposed scheme and (2) using the proposed blockchain-based secure PS system. Among them, the time overhead of the prototype system is from the time the subscriber initiates the subscription request until the subscriber successfully obtains the publishing service or data. Our scheme would consist the additional time spent in running BPAC. This paper evaluates the proposed scheme in terms of the different event sizes of a publish event, the number of different policies, and the number of attributes of a subscriber, where the number of policies is 1, 2, 4, 6, and 8, and the number of attribute values is 1, 5, 10, 15, and 20. In addition, in order to better verify the efficiency of the proposed scheme, we compare our scheme with the CACF [22] scheme under the same test environment, which is a comprehensive access control framework using FHE scheme for publish/subscribe-based IoT services communication. The specific experimental results are shown as follows. It is worth noting that all data were obtained after running 100 times.

As is shown in Figure 6(a), with the publishing event sizes increases, the system delay gradually increases; that is, the size of the data event is one of the main factors that affect PS system latencies. Among them, the delay of the prototype system is significantly lower than our proposed scheme, and the CACF scheme is slightly higher than the prototype system but significantly lower than our scheme. This is due to the fact that the consensus validation process in our scenario consumes part of time and increase with the event complexity. Figure 6(b) shows the average sustainable throughput in processing the publishing events per second using different event sizes. Node that the throughput results are based on

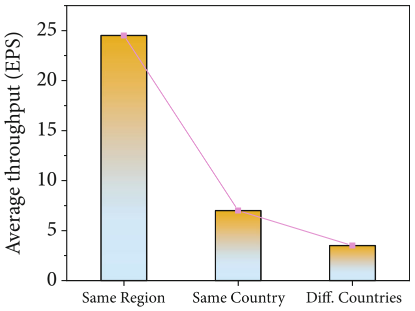

Figure 8: Throughput of query with nodes in different locations.

the average system latencies with or without our BPAC mechanism. As is shown in Figure 6(b), the system throughput decreases with the growth of data event sizes; that is to say, fewer the publishing events per second can be sent from the publisher to subscriber. In addition, we can know from the above two figures that the moderate amount of event data can complete PS service with low latency and acceptable throughput.

Figure 7 shows the impact on the system time overhead from both publisher and subscriber factors, where we mainly consider how the number of policies in one publishing event and attributes in one subscriber affect PS system latencies. In Figure 7(a), an increase in the number of subscriber attributes will result in an increase in the system time latency. This is because an increase in the number of attributes directly lead to more time in the attribute filtering and access control policy enforcement phases. Among them, the CACF scheme is still slightly lower than the scheme we proposed, which is because the FHE algorithm used in our scheme increases the time overhead. As shown in Figure 7(b), with the increase of access control policies, the time delay of the system gradually increases, and the delay of our scheme is about 43~50 ms. The time cost of the prototype system is significantly lower than ours, while CACF scheme is slightly higher than the prototype system but lower than our scheme. This is because our solution consumes part of the time and grows as the number of access control policies increases.

In Figure 8, in order to reflect the efficiency of crossdomain access operations, we test the throughput of our proposed PS system in different scenarios. All the experimental data is collected based on a minimum crossdomain access requirement that only involves one global ledger and two edge ledgers, and the average throughput in processing events per second is based on one KB event size. It is clear from Figure 8 that the physical location of the nodes also affects the performance of the PS system.

As can be seen from the results discussed above, although our proposed BPAC mechanism increases the system time delay compared with the CACF scheme, the absolute value of the delay increment is not large, and the application of blockchain in the PS system makes up for the lack of security and trust in the traditional scheme. We compromised the acceptable response time in exchange for higher reliability and solved the security problem in the PS system.

## 6. Conclusion and Future Work

In this paper, we propose an access control mechanism based on blockchain and FHE algorithm, which solves the security and privacy problems in the traditional centralized PS system. Our scheme protects the confidentiality of event data by encrypting the publishing data with the FHE algorithm. Meanwhile, it replaces the traditional central broker with the blockchain technology to realize decentralized distributed access control and realizes crossdomain information interaction by storing data in the global ledger. According to the theoretical analysis, it can guarantee the security and correctness of the system, and the experimental results show that our scheme is feasible and efficient to some extent.

However, our scheme also has certain deficiencies, such as our solution did not completely realize attribute revocation and update of access policies, and with the rapid growth of the IoT network scale, the attributes of one subscriber and access control policies for publishing events also become increasingly complex, as it may take more time in the matching stage, so as to further prolong system response time. In future research work, we will further solve the above problems. We plan to combine the two-strategy attribute-based authorization [33] and time-limited key management to realize more fine-grained access control and efficient key revocation and further adopt the Bloomer Filter [34] to optimize the matching process to achieve fast authentication.

## Notations

| | |
|---|---|
| $\lambda$: | Security parameter |
| $L$: | A number of levels |
| $b$: | Bit |
| $q$: | Prime |
| Params : | System parameter |
| $(\mathrm{PK}_p, \mathrm{SK}_p)$: | The key pair of publisher |
| $(\mathrm{PK}_S, \mathrm{SK}_S)$: | The key pair of subscriber |
| $r_{\mathrm{pp}}, r_{\mathrm{up}}, r_{\mathrm{ac}}$: | Random number |
| $h$: | Hash function |
| $e_{\mathrm{tp}}$: | Publishing event |
| tp: | Topic |
| $\Lambda_{\mathrm{tp}}$: | Access policy |
| $C_{\mathrm{tp}}$: | The ciphertext of the publishing event |
| $A_{\mathrm{im}}$: | Attribute collection |
| $F$: | Attribute filter function |
| $\omega_{\mathrm{topic}}$: | Access credentials |
| $j$: | Property index value |
| $I$: | The ciphertext of property index value |
| $\omega_s$: | Attribute conjunction |
| $\mathrm{KS}_{P\longrightarrow S}$: | The exchanged key |
| $\mathrm{EL}_i$/GL: | Edge ledger/global ledger. |

## Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

## Disclosure

A preprint has previously been published [35].

## Conflicts of Interest

The authors declare no conflicts of interest.

## Acknowledgments

This work was supported by the State Grid Liaoning Electric Power Supply Co., Ltd (No. 2022YF-22).

## References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[2] F. Javed, M. K. Afzal, M. Sharif, and B. S. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: a comparative review," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] Y. A. Younis, K. Kifayat, and M. Merabti, "An access control model for cloud computing," *Journal of Information Security and Applications*, vol. 19, no. 1, pp. 45–60, 2014.

[5] "Ericsson mobility report," 2020, https://www.ericsson.com/en/internet-of-things.

[6] L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, and R. Fujdiak, "A secure publish/subscribe protocol for internet of things," in *Proceedings of the 14th international conference on availability, reliability and security*, pp. 1–10, Canterbury CA UK, 2019.

[7] C. Esposito and M. Ciampi, "On security in publish/subscribe services: a survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 966–997, 2014.

[8] A. V. Uzunov, "A survey of security solutions for distributed publish/subscribe systems," *Computers & Security*, vol. 61, pp. 94–129, 2016.

[9] A. Banks and R. Gupta, "MQTT version 3.1.1," 2014, OASIS Standard, http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html.

[10] D. Hughes, K. Thoelen, W. Horré et al., "LooCI: a loosely-coupled component infrastructure for networked embedded systems," in *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia*, pp. 195–203, Kuala Lumpur Malaysia, 2009.

[11] P. A. Levis, S. Madden, D. Gay et al., "The emergence of networking abstractions and techniques in TinyOS," *NSDI*, vol. 4, pp. 1–1, 2004.

[12] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," 2009, https://metzdowd.com.

[13] J. Golosova and A. Romanovs, "The advantages and disadvantages of the blockchain technology," in *IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)*, pp. 1–6, Vilnius, Lithuania, 2018.

[14] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, "(leveled) fully homomorphic encryption without bootstrapping," *ACM Transactions on Computation Theory*, vol. 6, no. 3, pp. 1–36, 2014.

[15] J. Ren, Y. Pan, A. Goscinski, and R. A. Beyah, "Edge computing for the Internet of Things," *IEEE Network*, vol. 32, no. 1, pp. 6-7, 2018.

[16] A. V. Dastjerdi and R. Buyya, "Fog computing: helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[17] H. Tian, X. Ge, J. Wang, C. Li, and H. Pan, "Research on distributed blockchain-based privacy-preserving and data security framework in IoT," *IET Communications*, vol. 14, no. 13, pp. 2038–2047, 2020.

[18] P. T. Eugster, P. A. Felber, R. Guerraoui, and A. M. Kermarrec, "The many faces of publish/subscribe," *ACM computing surveys (CSUR)*, vol. 35, no. 2, pp. 114–131, 2003.

[19] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1767–1777, 2018.

[20] "Hyperledger Fabric," 2020, https://www.hyperledger.org/projects/fabric.

[21] E. Androulaki, A. Barger, V. Bortnikov et al., "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, pp. 1–15, Porto Portugal, 2018.

[22] L. Duan, C. A. Sun, Y. Zhang, W. Ni, and J. Chen, "A comprehensive security framework for publish/subscribe-based IoT services communication," *IEEE Access*, vol. 7, pp. 25989–26001, 2019.

[23] K. Yang, K. Zhang, X. Jia, M. A. Hasan, and X. S. Shen, "Privacy-preserving attribute-keyword based data publish-subscribe service on cloud platforms," *Information Sciences*, vol. 387, pp. 116–131, 2017.

[24] Q. Wang, D. Chen, N. Zhang, Z. Ding, and Z. Qin, "PCP: a privacy-preserving content-based publish–subscribe scheme with differential privacy in fog computing," *IEEE Access*, vol. 5, pp. 17962–17974, 2017.

[25] A. A. Diro, N. Chilamkurti, and N. Kumar, "Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing," *Mobile Networks and Applications*, vol. 22, no. 5, pp. 848–858, 2017.

[26] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman, and Y. Nam, "Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication," *IEEE Access*, vol. 8, pp. 60539–60551, 2020.

[27] C. Borcea, Y. Polyakov, K. Rohloff, and G. Ryan, "PICADOR: end-to-end encrypted publish-subscribe information distribution with proxy re-encryption," *Future Generation Computer Systems*, vol. 71, pp. 177–191, 2017.

[28] Y. Zhao, Y. Li, Q. Mu, B. Yang, and Y. Yu, "Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, 2018.

[29] P. Lv, L. Wang, H. Zhu, W. Deng, and L. Gu, "An IoT-oriented privacy-preserving publish/subscribe model over blockchains," *IEEE Access*, vol. 7, pp. 41309–41314, 2019.

[30] M. A. Tariq, B. Koldehofe, and K. Rothermel, "Securing broker-less publish/subscribe systems using identity-based encryption," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 518–528, 2014.

[31] G. S. Ramachandran, K. L. Wright, L. Zheng et al., “Trinity: a byzantine fault-tolerant distributed publish-subscribe system with immutable blockchain-based persistence,” in *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 227–235, Seoul, Korea (South), 2019.

[32] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, “TrustAccess: a trustworthy secure Ciphertext-policy and attribute hiding access control scheme based on Blockchain,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5784–5798, 2020.

[33] L. Duan, Y. Zhang, S. Chen, S. Wang, B. Cheng, and J. Chen, “Realizing IoT service’s policy privacy over publish/subscribe-based middleware,” *Springerplus*, vol. 5, no. 1, 2016.

[34] R. Barazzutti, P. Felber, H. Mercier, E. Onica, and E. Riviere, “Efficient and confidentiality-preserving content-based publish/subscribe with prefiltering,” *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 3, pp. 308–325, 2017.

[35] H. Tian, X. Ge, J. Wang, and C. Li, “Exploiting blockchain and secure access control scheme to enhance privacy-preserving of IoT publish-subscribe system,” *Research Square*, 2021.