ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

Privacy Preserving In IoT While Data Sharing Based On Blockchain

Shabeena A*[1], D. K. Kalaivani[2]

[1, 2] Department of Computer science and engineering, Udaya School of engineering, Udaya nagar, Vellamodi, Kanyakumari Tami nadu, India.

*sabi2kx@gmail.com

ABSTRACT

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, 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 in PS system can efficiently achieve the equilibrium between the system cost and the security requirement.

Keywords: Internet of Things, Post Script, User Interface, Radio waves

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. It was estimated that there will be over 24.9 billion IoT devices connected to the Internet by 2025. 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. Thus, 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. 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. The original publish-subscribe model relies on a trusted third-party broker such as MQTT, LooCI, and NesC, where data from all devices flows to subscribers through a central broker.

2 Related work

Zhao et al[1]. 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 pseudo anonymity 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. Lv et al[2]. 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. [3] 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.

3 Proposed Methodology

In this paper, use additional security model to protect the data transfer and privacy preserving**.** Other than just getting the ciphertext as in the existing system, this paper would generate an additional authentication named Ring Signature with other public keys before each transfer or a transaction. By this way, the system could identify weather the request is made by the actual DU or from a MCU using the Disoval algorithm**.** Data is transferred or a reward is rewarded only if the system finds authenticity in the user request.

3.1 Pre-processing

Blockchain is a peer-to-peer distributed ledger technology that provides a shared, immutable, and transparent append-only register of all the actions that have happened to all the participants of the network. It is secured using cryptographic primitives such as hash function, digital signature, and encryption

3.2 Segmentation

3.2.1 BPAC System Model

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

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

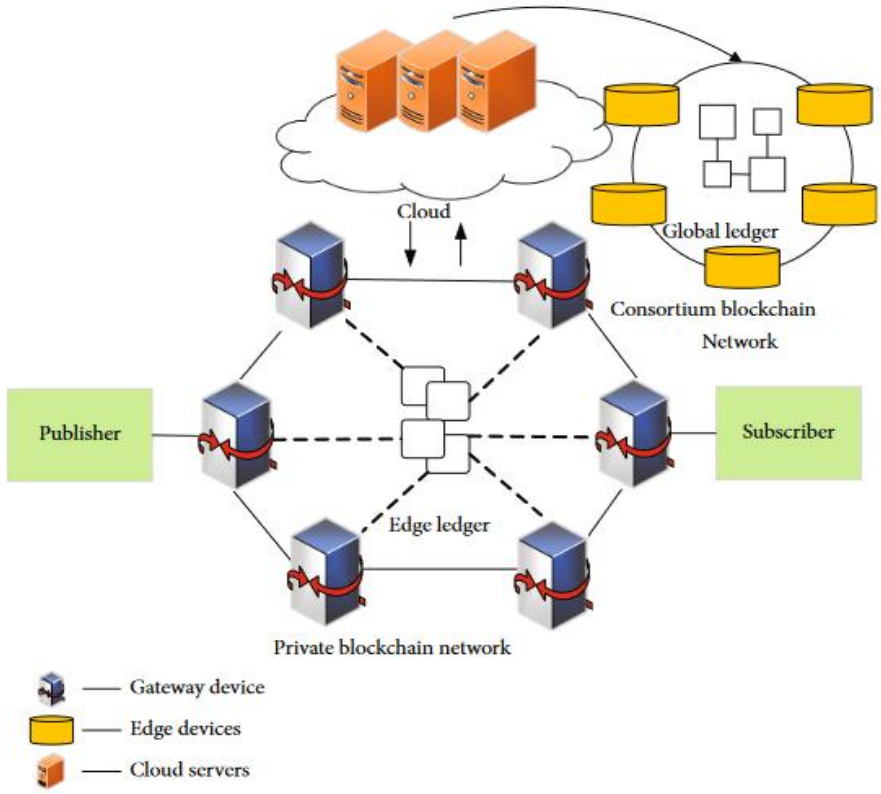

Figure 1: *Security access control system model*

3.2.2 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 this scheme, publishers and sub- scribers within the domain directly interact with each other through private blockchain, and the crossdomain users connect private blockchain through consortium blockchain for temporary cross domain 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 a framework system model.

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

3.2.3 Setup

The setup algorithm takes the security parameter λ, a number of levels L, and b ∈ f0, 1g as input parameters to generate the system parameter Params = (q, d, n, N, χ). This algorithm is run by CA, and only CA knows the value of Params, where let μ = μ(λ, L, b), whose modulus is prime q, and d = d(λ, μ, b), n = n(λ, μ, b), N = N(λ, μ, b), and χ = χ(λ, μ, b).

Finally, the key pair PK and SK are generated as follows:

$$\text{SecretKeyGen(params)} \longrightarrow \text{SK},$$
$$\text{PublicKeyGen(params)} \longrightarrow \text{PK}, \quad (1)$$

where the key pair of publisher and subscriber is, respec- tively, (PKp, SKp) and (PKS, SKS). The publisher randomly selects random num-ber rpp, rup, rac and hash function h in advance, where rpp is greater than the number of topics in the publishing event etp, then generates hup = h(Ai1kAi2k ⋯ kA imkrup), and encrypts event etp with topic tp and policy Λtp = (A 11ΛA12Λ ⋯ ΛA 1t (V)As1ΛAs2Λ ⋯ Ast) as Ctp through edge servers. For each set of attribute conjunction formula Ai1 Λ Ai2 Λ ⋯ ΛAim(1 ≤ i ≤ n), the publisher generates F s through the attribute filter function F(Ai1 Λ ⋯ Λ Aim), uses the edge servers.

The publisher randomly selects random number rpp , rup , rac and hash function h in advance, where rpp is greater than the number of topics in the publishing event etp, then generates hup = h(Ai1kAi2k ⋯ kA imkrup), and encrypts event etp with topic tp and policy Λtp = (A 11ΛA12Λ ⋯ Λ A 1t)V(As1ΛAs2Λ ⋯ Ast) as Ctp through edge servers. For each set of attribute conjunction formula Ai1 Λ Ai2 Λ ⋯ ΛAim (1 ≤ i ≤ n), the publisher generates F s through the attribute filter function F(Ai1 Λ ⋯ Λ Aim), uses the edge servers to convert it into access credentials:

$$\omega\text{topic} = (\text{KSP} \longrightarrow \text{S}, \{(\text{C11}, \text{C12}, \text{F1}), (\text{C21}, \text{C22}, \text{F2}), \cdots, (\text{Cs1}, \text{Cs2}, \text{Fs})\}$$
$$\{(\text{C13}, \text{C14}), (\text{C23}, \text{C24}), \cdots, (\text{Ch3}, \text{Ch4})\} \quad (2)$$

and finally publishes F s and C tp on a private blockchain. The encryption process for publishing events is as follows:

$$\text{C i1} = \text{Encrypt (SKP, rup)},$$
$$\text{C i2} = \text{Encrypt (SKP, hup} + \text{rpp} - \text{rac (h (Ai1)} + \text{h (Ai2)} + \cdots + \text{h (Aim))}),$$
$$\text{C j3} = \text{Encrypt (PK S, r S)},$$
$$\text{Cj4} = \text{Encrypt (PK S, h v} + \text{rac (h A j1 }') + (\text{h A j2 }') + \cdots + \text{h (A jm }') \quad (3)$$

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.

3.2.4 Match and Key Switching

When the publisher receives a subscription request from the subscriber, it first checks whether subscriber's attribute conjunction ωs satisfies ωs ∈ 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 ′, C1, C s. The conversion process is as follows:

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

$$Ctp' = ReEncrypt(KSP \longrightarrow S, Ctp) = Encrypt(PK\ S, etp + rpp * r),$$
$$C1 = ReEncrypt(KSP \longrightarrow S, C\ i1) = Encrypt(PKs, r\ ac),$$
$$CS = ReEncrypt(KSP \longrightarrow S, C\ i2) \oplus C\ j4 = Encrypt(PKS, rpp + hup + hv) \quad (4)$$

Finally, the publisher authorizes the subscriber S to access C tp ′, C1, 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.

3.2.5 Receive

After subscriber S receives C tp ′, C1, C s, I and C j3, it first decrypts I to obtain index j, thus obtaining the authorization attribute conjunction ωj = A j1 ′Λ A j2 ′Λ ⋯ Λ A jm ′. Then it decrypts C j3 and C1 to get the random values r s and r ac. Then, the subscriber uses hash function h to restore rpp:

$$hup = h(Aj1'\ Aj2'\ \cdots\ Ajm'\ rup),$$
$$hv = h(Aj1'\ Aj2'\ \cdots\ Ajm'\ r\ S),$$
$$rpp = Decrypt(SKS, C\ S) - hup - h\ v: \quad (5)$$

Finally, the subscriber decrypts the ciphertext Ctp ′ and gets etp + rpp ∗ r, and the modular operation is then per- formed on rpp to recover the event etp.

3.2.6. 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 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 EL 1 and EL 2 are two subscribers of edge ledger in different domains. EL 1 needs to access the publishing events in EL 2 through the global ledger GL and verifies its validity.

- EL 2 processes the new authorization information block tx.
- EL 1 initiates a verification request for information block tx to the global ledger GL. GL forwards it to EL 2 and EL 2 initializes the value acc of the accumulator after receiving the verification request
- EL 2 packs tx into a new block blk and updates the accumulator value to acc′
- All nodes el 2j in EL 2 run the consensus protocol to add blk and update accumulator value acc′ to the blockchain
- EL 2 updates its status to GL
    - EL 2 only updates the accumulator value to GL after a certain number of new blocks are created
    - GL checks whether EL 2 has achieved consensus on acc′, if it passes the check, then the latest state of (EL 2 , acc′) is included in the new block
- EL 1 checks the validity of tx
    - EL 1 obtains the current accumulator value of EL 2 from GL
    - EL 1 requests EL 2 to provide evidence that block blk contains the authorization information block tx

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

- EL 2 responses to EL 1's request and provides a proof that blk is included in the edge ledger EL 2 EL 1 verifies the evidence. After verification, it can utilize the information in text.

4 System architechture

In order to verify the availability and performance of our proposed BPAC mechanism, deployed the 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, use the Hyperledger Fabric deployed on the IBM Cloud platform for the consortium blockchain. Here, use system throughput and two types of time delay as the main performance.

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

In this is system delay with different numbers of attributes and policies:

(i) latency with different numbers of attributes on one subscriber

(ii) Latency with different numbers of policies in one event.

Evaluation criteria: PS prototype system without using the proposed scheme and 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.

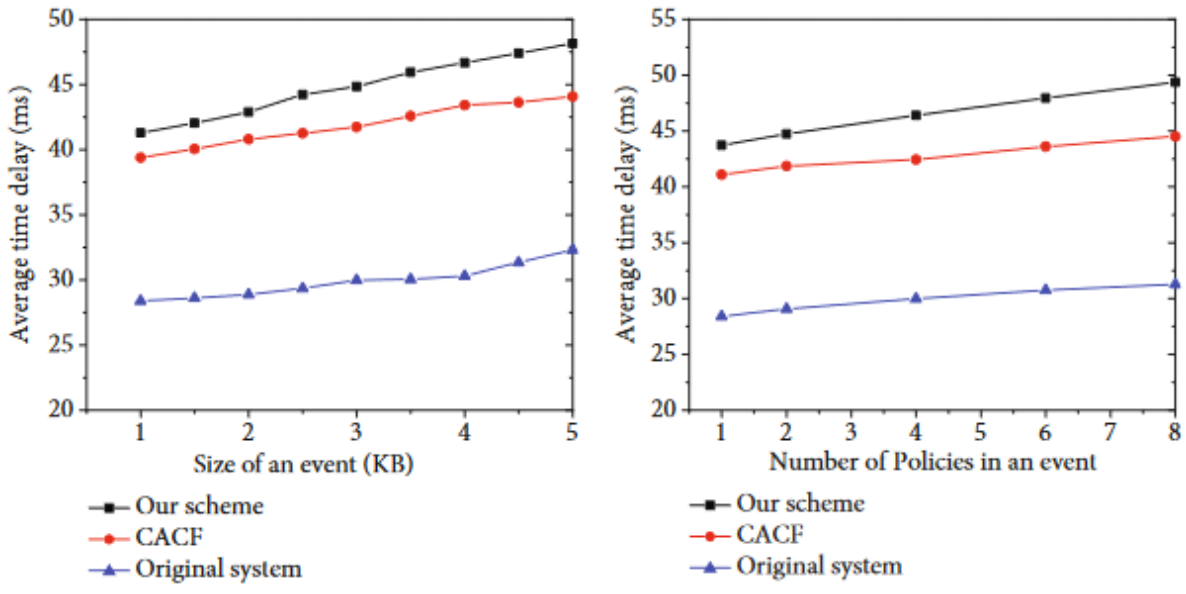

Figure 2: *System delay and throughout architecture*

ISSN (Online): 2583-7052

International Journal of Advanced Trends in Engineering and Management (IJATEM)
pp. 66-74

Article Title: Privacy Preserving In IoT While Data Sharing Based On Blockchain

4.1 Feature Extraction

Blockchain transactions allow users to control their data through private and public keys, allowing them to own it. Third-party intermediaries are not allowed to misuse and obtain data. If personal data are stored on the blockchain, owners of such data can control when and how a third party can access it.

4.2 Classification

4.2.1 Query with nodes

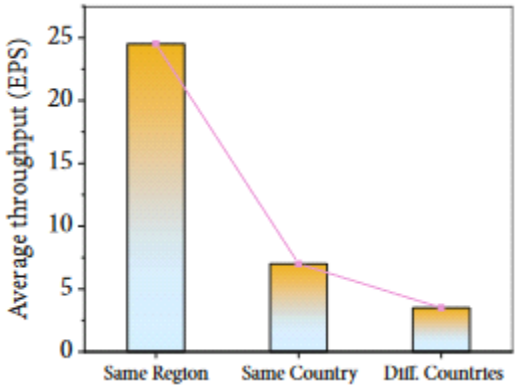

Figure 3: *Query with node*

Node that the throughput results are based on the average system latencies with or without our BPAC mechanism. As is shown in Figure, the system through- put 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, 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 this scheme increases the time overhead. As this paper, 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 this scheme. This is because of solution consumes part of the time and grows as the number of access control policies increases.

5 Result and Discussion

This module constantly interprets the client or End User request with the UUID. This module classifies the requests either a valid or invalid request. The Malicious Cloud User is identified using Disoval algorithm if the request is found to be from the MCU, the system would abort the transaction request to the server. And waits for a successful transaction initiation. Once the request was successful, the system verifies the token which was returned during the upload process. Furthermore we use RING signature to ensure the verification. If everything is fine, the Cloud User is rewarded for their token. Once the rewarding is successful, the system resets UUID, tokens and OAUTH 2.0 tokens.

6 Conclusion

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.

Reference

1. Jie Xu; Kaiping Xue; Shaohua Li; Hangyu Tian; Jianan Hong; Peilin Hong; Nenghai Yu, Year: 2019, “Healthchain: A blockchain-based privacy preserving scheme for large-scale health data”, IEEE Internet Things J., Vol: 6, no: 5, pp. 8770–8781.

2. Philip Alexander Levis; Samuel Madden; David Gay; Joseph Polastre; Robert Szewczyk; Alec Woo; Eric A. Brewer; David E. Culler, Year: 2004, “The emergence of net-working abstractions and techniques in TinyOS”, NSDI, Vol: 4, pp. 1 – 1.

3. Yanqi Zhao; Yannan Li; Qilin Mu; Bo Yang; Yong Yu, Year: 2018, “Secure pub-sub: blockchain-based fair payment with reputation for reliable cyber physical systems”, IEEE Access, Vol: 6, pp. 12295 – 12303.

4. Ali Hassan Sodhro; Sandeep Pirbhulal; Arun Kumar Sangaiah, Year: 2018, “Convergence of IoT and product lifecycle management in medical health care”, Future Gener. Comput. Syst., Vol: 86, pp. 380 – 391.

5. Anton V. Uzunov, Year: 2016, “A survey of security solutions for distributed publish/subscribe systems”, Computers & Security, Vol: 61, pp. 94 – 129.

6. Abebe Abeshu Diro; Naveen Chilamkurti; Neeraj Kumar, Year: 2017, “Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing”, Mobile Networks and Applications, Vol: 22, no: 5, pp. 848 – 858.

7. Abebe Diro; Haftu Reda; Naveen Chilamkurti; Abdun Mahmood; Noor Zaman; Yunyoung Nam, Year: 2020, "Lightweight authenticated-encryption scheme for internet of things based on publish-subscribe communication", IEEE Access, Vol: 8, pp. 60539 – 60551.

8. Cristian Borcea; Yuriy Polyakov; Kurt Rohloff; Gerard Ryan, Year: 2017, "PICADOR: end-to-end encrypted publish-subscribe information distribution with proxy re-encryption", Future Generation Computer Systems, Vol: 71, pp. 177 – 191.

9. Danny Hughes; Klaas Thoelen; Wouter Horré; Nelson Matthys; Javier Del Cid; Sam Michiels; Christophe Huygens; Wouter Joosen, Year: 2009, "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. 195203.

10. Deepak Puthal; Surya Nepal; Rajiv Ranjan; Jinjun Chen, Year: 2011, "Threats to networking cloud and edge datacenters in the Internet of Things", IEEE Cloud Comput., Vol: 3, no: 3, pp. 64 – 71.