Cluster Computing (2021) 24:1331–1345
https://doi.org/10.1007/s10586-020-03190-3

Privacy protection for fog computing and the internet of things data based on blockchain

Yanhui Liu[1,2] · Jianbiao Zhang[1,2] · Jing Zhan[1,2]

Received: 15 May 2020 / Revised: 30 September 2020 / Accepted: 6 October 2020 / Published online: 15 October 2020

Abstract
With the development of the Internet of Things (IoT) field, more and more data are generated by IoT devices and transferred over the network. However, a large amount of IoT data is sensitive, and the leakage of such data is a privacy breach. The security of sensitive IoT data is a big issue, as the data is shared over an insecure network channel. Current solutions include symmetric encryption and access controls to secure the data transfer, but they have some drawbacks such as a single point of failure. Blockchain is a promising distributed ledger technology that can prevent the malicious tampering of data, offering reliable data storage. This paper proposes a distributed access control system based on blockchain technology to secure IoT data. The proposed mechanism is based on fog computing and the concept of the alliance chain. This method uses mixed linear and nonlinear spatiotemporal chaotic systems (MLNCML) and the least significant bit (LSB) to encrypt the IoT data on an edge node and then upload the encrypted data to the cloud. The proposed mechanism can solve the problem of a single point of failure of access control by providing the dynamic and fine-grained access control for IoT data. The experimental results of this method demonstrated that it can protect the privacy of IoT data efficiently.

Keywords Blockchain · IoT · Access control · Data privacy · Cloud storage

1 Introduction

The Internet of things is an emerging technology. Owing to the accompanying growth of IoT, a great deal of attention has focused on the issues of IoT devices [1]. IoT is a system of interconnected computing devices with unique identifiers (UIDs) and can perform data communications without any human involvement. The definition of the IoT has evolved due to the convergence of multiple technologies in it, such as real-time analytics, machine learning, commodity sensors, and embedded systems. The term "things" refers to intelligent and self-configurable devices. These devices are used to build efficient and dynamic platforms for communication and collaboration [2]. The devices used in IoT are heterogeneous and resource-constrained in terms of storage, power, and computation. According to a study published by Gartner, the number of connected devices in IoT will rise to 20 billion by the year 2020 [3]. However, there are several serious concerns raised due to the growth of IoT [4], especially in the areas of privacy and security of data. Consequently, the governments and industry have started taken moves to address these concerns.

The high-level architecture of IoT is shown in Fig. 1. It consists of the sensing/perception layer, networking layer, middleware layer, application layer, and business layer [5]. The perception layer deals with sensor devices. These devices sense data from the physical world and communicate it to the middleware layer through the network layer. The network layer uses different technologies such as 4G, 5G Bluetooth, and ZigBee for the transmission of the data

✉ Yanhui Liu
yanhui1999@bjut.edu.cn

✉ Jianbiao Zhang
zjb@bjut.edu.cn

Jing Zhan
zhanjing@bjut.edu.cn

[1] Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

[2] Beijing Key Laboratory of Trusted Computing, Beijing 100124, China

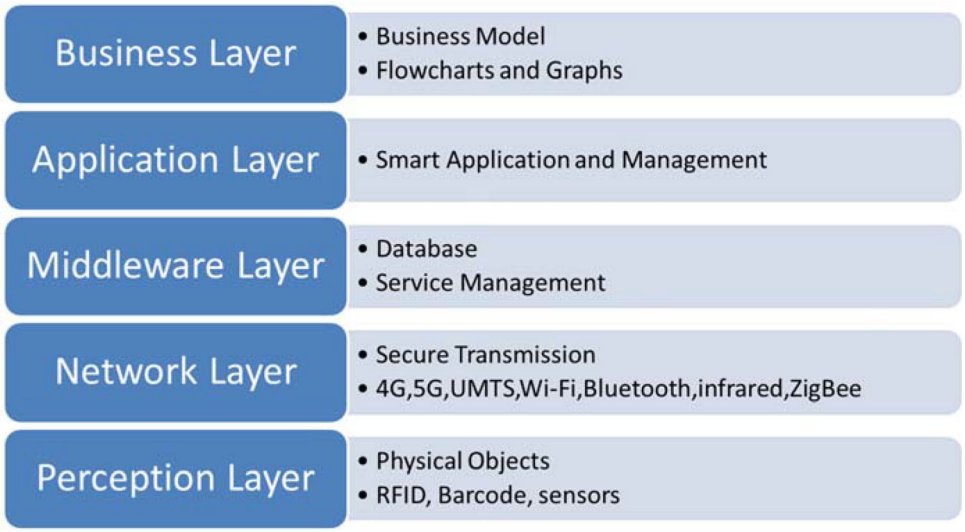


Fig. 1 Architecture of IoT

to the middleware layer. The middleware layer uses a database to store all the data from sensors. The application layer collects the data from the middleware layer and integrates it with smart apps. Finally, the business layer is responsible for the management of the whole IoT system and services.

IoT devices generate a huge amount of data, some of which may be sensitive. For example, in the smart healthcare system [6], the data generated by the IoT devices is related to the personal health status of patients, which is very confidential. Thus, it is important to protect these devices and sensitive data from any security breach. Access control is the first line of defense, which limits the data access to only those having the correct permissions [7]. Encryption is also a good option for data security to ensure data confidentiality and integrity. Without a proper security mechanism, sensitive data can be vulnerable to various forms of attack.

Access controls and data privacy are indispensable means to achieve secure communication in an IoT network [8, 9]. However, due to the resource-constrained nature of IoT devices, conventional mechanisms are not suitable for this complicated system. For example, in centralized mechanisms such as the ones proposed in [10], there are problems of scalability, single point of failure, and are highly prone to security threats during communication. To overcome these issues, a decentralized mechanism was proposed in [11], but it still has limited scope in communication. There is a need for a new mechanism that is more suitable for the distributed nature of the IoT system.

In recent years, blockchain technology has attracted significant scientific interest in research areas, one of them being the Internet of Things [12]. The blockchain technology can be an effective solution for fog computing and IoT problems [13–19], mainly due to its decentralized nature and cryptographic properties. Blockchain allows the integration of access controls that offer a fine-grained access control mechanism for IoT devices. Benefiting from the characteristics of fog computing and the distributed nature of blockchain, we have proposed a blockchain-enabled access control mechanism for the security of IoT systems. The main contributions of this paper are summarized below:

- A novel decentralized mechanism that provides fine-grained access control to create a controlled and secure environment for IoT systems.
- A secure data sharing mechanism for IoT systems by using mixed linear-nonlinear coupled map lattice and least significant bit method algorithm.
- The effectiveness of the proposed method was demonstrated with the case study using IoT data sharing for a smart city, followed by a security analysis and comparison with the state-of-the-art blockchain-based access control techniques.

The remainder of this paper is organized as follows: Sect. 2 describes the background of our research. Section 3 presents the related work. Section 4 explains our decentralized blockchain-based mechanism. The experimental setup, case study demonstration, security analysis, and comparative analysis are presented in Sect. 5. Finally, Sect. 6 concludes the paper and identifies some future work.

2 Background

This section provides an overview of the blockchain technology, the least significant bit method algorithm, mixed linear-nonlinear coupled map lattice, and attribute-based access control mechanisms.

2.1 Blockchain

Bitcoin was first introduced by Nakamoto (a pseudonym of Satoshi Nakamoto) in a review of the cryptography group "Bitcoin: A Peer-to-Peer Electronic Cash System [20]" in 2008. The article described an electronic cash system based on peer-to-peer technology that can implement online payment functions without the participation of any intermediate financial institutions. It proposed a solution for avoiding double spending, called proof of work (PoW) mechanism.

When bitcoin was first proposed, it did not attract much attention. However, with its stable operations and development of the network, bitcoin is now popular worldwide. The underlying technology of bitcoin has gradually been noticed economy-wide. Authoritative magazines, like The Economist, Harvard Business Weekly, and Fox Magazine, have stated that blockchain technology will change the world. In 2017, the State Council issued the "National Technology Transfer System building programs" addressed the speed up the transfer of scientific and technological achievements of blockchain. Later, Gartner listed blockchain technology as one of the ten major strategic Science and Technology developments for 2018.

There is no universal definition for blockchain technology, but a blockchain is generally described as a special data structure formed by combining data blocks in a chain of chronological order along with a protocol that guarantees its cryptographic properties like tamper-proof data. The protocol is decentralized and creates a trust-free distributed shared ledger system. From a technical perspective, blockchain is a series of distributed ledger technologies implemented using a deep integration [21] of the P2P network, asymmetric encryption, consensus mechanism, and on-chain scripts techniques. The basic framework of the blockchain is shown in Fig. 2. It is mainly composed of a data layer, a network layer, a consensus layer, and an application layer. Blockchain technology utilizes an encrypted chain of blocks structure to verify and store data. P2P network technology and consensus mechanisms are used to implement distributed node verification, communication, and the establishment of trust relationships. On-chain script technology is used to implement complex business logic functions and automate the operation of the data, resulting in a new method of data recording, storage, and expression.

Blockchain technology has the following characteristics:

1. *Decentralization* There is no centralized management for blockchain nodes. All the participating nodes in blockchain perform network maintenance functions to maintain the network. Each node has equal status, and the damage of one/few node(s) will not affect the operation of the entire system;
2. *Trust-free* Nodes do not need to rely on trusted third parties to establish trust relationships between them in advance. As long as they operate according to the blockchain protocol, trusted collaboration and interaction can be accomplished among the distributed nodes;
3. *Anonymity* The users in the blockchain only correspond to the public key address. Therefore, users can complete a transaction without revealing their real identities;
4. *Tamper-resistance* In a blockchain system, the connected blocks have a verification relationship. To tamper the data of a block, the entire chain of blocks needs to change, and it must be changed within a certain time. Therefore, the more nodes are in the system, the higher is the security of the blockchain;
5. *Traceability* The blockchain uses a block structure to store data adding a time dimension to it also. Each transaction on the block is cryptographically related to two adjacent blocks, thus any transaction is traceable;
6. *Programmability* The blockchain supports the development of services in the application-layer by on-chain scripts, and users can implement complex decentralized applications by building smart contracts.

2.2 Least significant bit method algorithms

Least Significant Bit (LSB) method uses the least significant bit in a digital carrier to hide information that needs to be encrypted. In a colorful image, each pixel is described by an 8-bit binary code, and for each pixel, when the least significant bit is removed, the effect on the overall image can be ignored. So the lowest bits of the pixels in the image can be used to hide secret information. This mechanism has a capability of hiding information, it is simple and easy to implement, and has little impact on the original carrier. However, due to the irreversibility of the LSB algorithm on the carrier, and a provided security mechanism, many scholars have proposed improved methods, such as in [22–24].

The works in [22, 23] focused on improving reversible data hiding methods by increasing their efficiency and capacity. Since the existing data hiding methods have been published publicly, if these methods are stolen by those

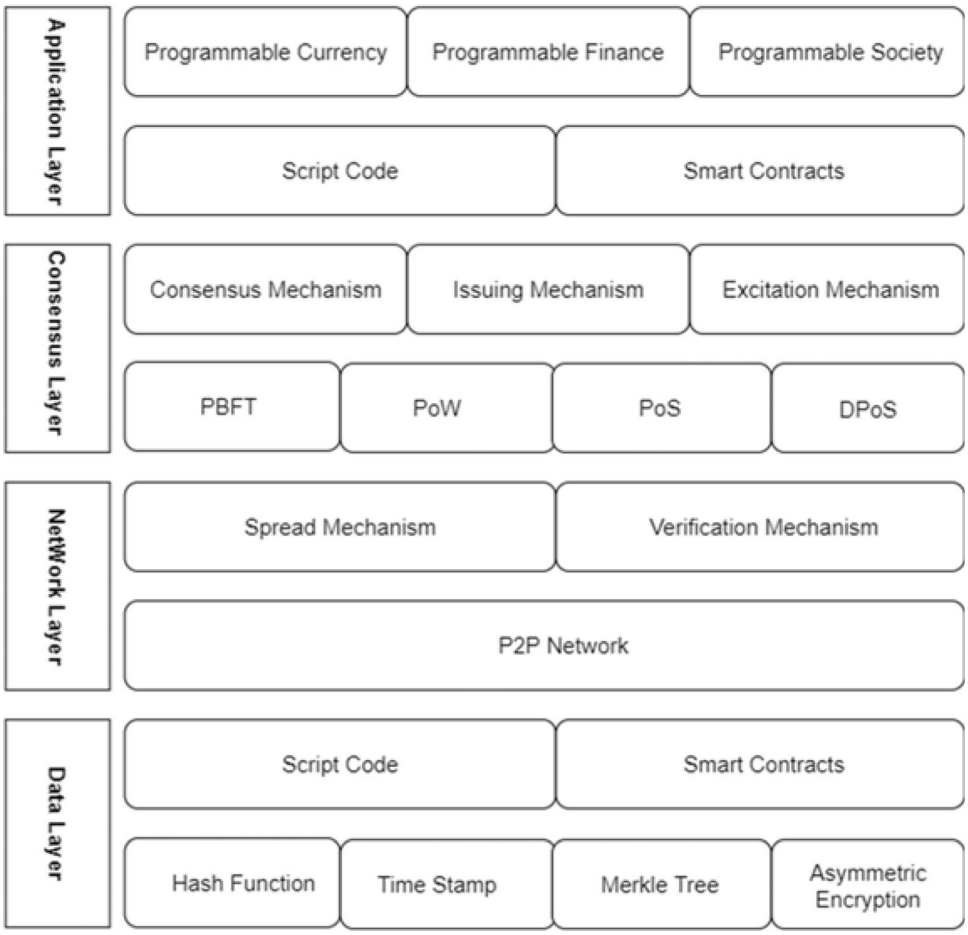


Fig. 2 Blockchain basic framework

having enough knowledge of these algorithms, then these methods cannot be called secure. To address this problem, scholars have proposed a method of hiding the data combined with the cryptography. This way, even if the stealer detects the image which contains the secret information, without having the correct key, the confidential information cannot be extracted.

2.3 Mixed linear-nonlinear coupled map lattice

In nature, non-linear motions exist widely, and spatiotemporal chaotic systems represent one of them [25, 26]. Since the coupled lattice model (CML) been proposed, many related works have made the coupled lattice model a mature theory. Kaige Zhu [25] design a color image encryption algorithm based on a chaotic system and block compressive sensing. Xingyuan Wang [26] proposed a novel spatiotemporal chaos model (McML) by mixing logistic, Sine, and tent maps into CML maps together.

Many scholars have researched chaotic systems in different fields [27, 28]. The logistic map [29] proposed by May is a first-order difference equation $f(x) = \mu x(1 - x)$. The mixed linear-nonlinear coupled map lattice (MLNCML) chaotic system is formed by the L logistic mapping system coupled through the spatial lattice point linear adjacent and spatial arnold cat mapping. The mathematical model is described below:

$$\begin{aligned} x_{n+1}(i) = {} & (1-\varepsilon) f[x_n(i)] \\ & + (1-\eta)\frac{\varepsilon}{2}\{f[x_n(i+1)] + f[x_n(i-1)]\} \\ & + \eta\frac{\varepsilon}{2}\{f[x_n(j)] + f[x_n(k)]\} \end{aligned} \tag{1}$$

where i, j, and k ($1 \le i, j, k \le L$) represent space lattice grids, $\varepsilon(0 \le \varepsilon \le 1)$ is the coupling coefficient, η $(0 \le \eta \le 1)$ is another coupling coefficient, and n (n = 1,2,3 …) is a time series and $f(x) = \mu x(1 - x)$, $\mu \in (0,4]$.

The lattice points between i, j and k are determined by the arnold cat mapping:

$$\begin{bmatrix} j \\ k \end{bmatrix} = A \begin{bmatrix} i \\ i \end{bmatrix} \mathrm{mod} L = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} i \\ i \end{bmatrix} (\mathrm{mod} L) \tag{2}$$

where p and q are mapping parameters. Different parameters p, q and η will lead to the different dynamic behavior of MLNCML system. When the parameters p, q, and η are set to fixed values, most of the spatial grids still have chaotic characteristics because the parameter μ changes

continuously. CML systems are suitable for encryption systems because their periodic windows are smaller than low-dimensional chaotic systems. The MLNCML system has a smaller periodic window than the CML system, so it is also suitable for encryption.

2.4 Attribute-based access control

Access control is a technology needed by almost all existing information systems. It refers to the technology that restricts the access of the subject to the object based on its identity and permissions (read, write, modify, execute, etc.), to ensure that data and resources are used within legal limits. Access control guarantees the confidentiality, integrity, and availability of data and resources. It is an important measure of system protection and security.

In an open network environment, the interactions between users and organizations, organizations and organizations, as well as multiple servers often lie between multiple different management domains, where the unified security access control policies cannot be deployed centrally. The attribute-based access control (ABAC) model provides a solution to this situation. In an ABAC model, resource requesters, resource owners, and access restrictions are all defined by attributes. Different entities in the system have different attributes, and access control policies can be processed uniformly based on those attributes. That is, in an open network environment, the identity of user doesn't have much impact, only the attributes related to the resource requester have proper worth. As long as the resource requester has the provided attributes, the system will grant the corresponding access rights to the requester. For the resource side, the relevant conditions and requirements for accessing the resource are generally fixed. So the appropriate methods can be used to organize these related conditions and requirements into related attributes. When the resource requester wants to access the resource, as long as the resource requester meets certain attribute requirements, which means the relevant access control policy is satisfied, the resource requester is allowed to access the resource. ABAC framework model is shown in Fig. 3 [30].

The components of the framework are described below:

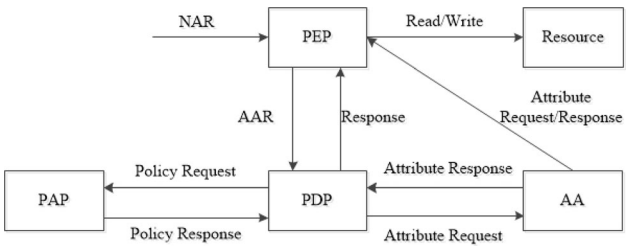


Fig. 3 ABAC basic framework

1. *Attribute-based Access Request (AAR)* Subject sends access requests based on the AAR;
2. *Policy enforcement point (PEP)* the main function is to establish AAR, send AAR to PDP, execute the decision result of PDP;
3. *The policy decision point (PDP)* whose main function is to check whether the subject in the AAR meets the policy rules and send the result back to the PEP for execution;
4. *Policy management point (PAP-Policy Authority Point)* which provides access control policies required for PDP decisions, PDP decision rules, basis, and related constraints are defined in the policy;
5. *Attribute Authority (AA)* is responsible for establishing and maintaining the subject, resource, and environmental attributes required by your organization or system.

The execution process of the ABAC model can be summarized as follow. First, the requester constructs the original request (NAR) and sends it to the policy enforcement point (PEP). The access request needs to contain information about the required subject, object, resource, current environment attributes, etc. Next, the policy enforcement point (PEP) receives the NAR and uses the information in the attribute authority (AA) and (NAR) to construct an attribute-based access request (AAR). Then, PEP sends AAR to Policy Decision Point (PDP). When the PDP obtains the policy from the policy management point (PAP), it checks the AAR, and finally sends the conclusion back to the PEP. The PEP performs inspection results, that is, access is allowed or prohibited.

Casbin is a powerful and efficient open-source access control framework. Its permission management mechanism supports multiple access control models. Casbin configures the permission model through a configuration file and divides a permission model into request policy, policy effect, and matches. Compared to XACML, Casbin is very simple. In ABAC, you can use struct (or a programming language-based class instance) instead of strings to represent model elements. At the same time, model elements can be formulated according to specific business access rules. Policy files can define detailed policies and the requests can include relevant attributes of access subjects and objects. The policy effect can determine the final judgment result based on the above elements. The result is to permit or to reject the request.

Casbin has the following characteristics:

1. Support for custom request formats. The default request format is {subject, object, action}.
2. Obeys access control model and strategic policy.

3. Supports multi-level role inheritance in RBAC. Not only the subject can have a role, but the resource can also have a role.
4. Supports super users, such as root or administrator. Super users can access any resource without being restricted by authorization policies.
5. Support a variety of built-in operators, such as key match, to facilitate the management of path-type resources, such as / foo / can be mapped to / foo *.

3 Related work

This section discusses some of the developed access control mechanisms proposed for IoT and privacy preservation.

Umair Khalid [7] proposed a decentralized authentication and access control mechanism for lightweight IoT devices and is applicable to many other applications. The mechanism is based on the technology of fog computing and the concept of a public blockchain. The results gained from the experiments demonstrate a superior performance of the proposed mechanism when compared to the state-of-the-art blockchain-based authentication techniques.

Bhabendu Kumar Mohanta [18] proposed a smart IoT system by using the Ethererum based blockchain system. Firstly, it reviewed and identified the security and privacy issue exists in IoT system. Secondly, blockchain technology provides some security solutions. The details analysis, including enabling technology and integration of IoT technologies, are explained. Lastly, a case study is implemented and the results are discussed.

Tehsin Kanwal [31] answered three major questions for privacy preservation in e-health cloud. Firstly, how privacy models and privacy techniques correlate with each other, secondly, how we can fix the privacy-utility-trade off by using different combinations of privacy models and privacy techniques and lastly, what are the most relevant privacy techniques that can be adapted to achieve privacy of EHR on cloud.

Soumya Banerjee [32] proposed a three-factor user access control scheme, which supports multi-authority ABE. This scheme is highly scalable as both the ABE key size stored in the user's smart card and cipher text size needed for authentication requests are constant with respect to the number of attributes.

Saqib Ali [33] designed a blockchain-based data storage and access framework for PingER (worldwide end-to-end Internet performance measurement project) to remove its total dependence on a centralized repository. In the proposed framework, metadata of the files are stored on the blockchain, whereas the actual files are stored off-chain through DHT at multiple locations using a peer-to-peer network of PingER Monitoring Agents.

Oscar Novo [34] proposed a new architecture for arbitrating roles and permissions in IoT. The new architecture is a fully distributed access control system for IoT based on Blockchain technology. The architecture is backed by a proof of concept implementation and evaluated in realistic IoT scenarios.

Shiping Fan [35] proposed an IoT information security protection scheme based on blockchain technology. The scheme utilizes the security features of the blockchain combined with the AES encryption algorithm to encrypt the original IoT information, and the cipher text distributed storage can effectively solve the IoT data storage problem.

Premanand Ghadekar [36] proposed a new lightweight and secure architecture for IoT using Ethereum Blockchain retaining most of its security providing powers. Since Blockchain is decentralized it solves the single point authentication problem existing in IoT networks. A Smart Home System as a representative case study has been implemented for broader IoT applications. The two parameters measured are temperature and intrusion detection. The proposed model tackles some more challenges that exist in IoT networks. The qualitative evaluation of the proposed architecture highlights how it outstand various attacks.

Yuta Nakamura [37] proposed a decentralized and trustworthy Capability-Based Access Control (CapBAC) scheme using the Ethereum smart contract technology. In this scheme, a smart contract is created for each object to store and manage the capability tokens (i.e., granted access rights for data structures recording) assigned to the related subjects, and also a verification of the ownership and validity of the tokens for access control.

4 Proposed mechanism

The main aim of this work is to provide a blockchain-based distributed access control system to maintain the IoT data privacy. In this section, we will discuss the system architecture of the proposed mechanism.

Figure 4 shows an example of a distributed IoT architecture that is suitable to provide dynamic and fine-grained access control. In this IoT architecture, multiple smart devices are formed in such a way to build a smart environment in which the devices are connected to the internet through the edge node(s). The resource requesters can access the services of the smart devices through the edge node(s) after completing an access control process. It is worth mentioning here, that a resource requester has all attributes defined under multiple smart environments at the same time.

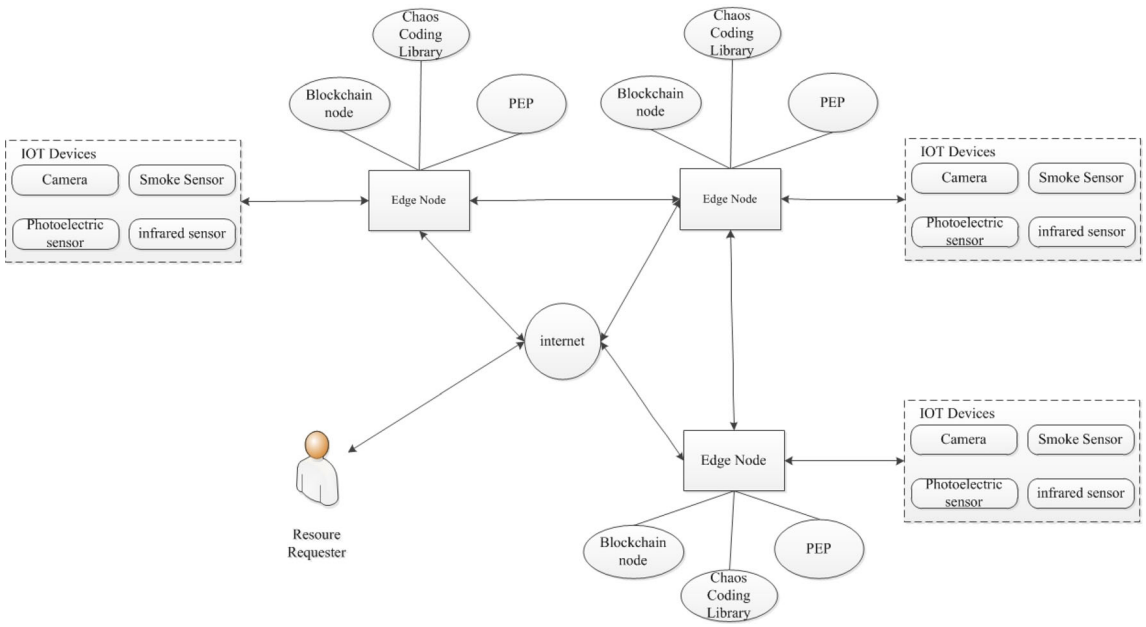


Fig. 4 The IoT architecture for distributed access control based on blockchain

In Fig. 4, each edge node is also a blockchain node. All the blockchain nodes form an alliance chain. The IoT device access control policy is store in the blockchain. Hence, the access control decision can be made by an edge node in a distributed manner.

In this paper, we propose an LSB image encryption system scheme combined with MLNCML. The proposed encryption scheme is described in Fig. 5. Firstly, the plaintext information is converted to Unicode encoding. Next, the chaotic series is used to encrypt the Unicode encoding to obtain encrypted information. The encrypted information is then made hidden in the original image through the LSB algorithm to obtain the encrypted image. Lastly, the MLNCML series is used to perform secondary encryption on the encrypted image to obtain the final encrypted image. The decryption process is the reverse of this process.

When encrypt an image, it follows the steps in Algorithm 1.

Algorithm 1 encryption(*plaintext, cs,ms, image*): steps to get an encrypt image

```
Input plaintext and assign it to plaintext
Convert plaintext to Unicode
Input chaotic sequences and assign it to cs
if run encrypt algorithm success then
   Get encrypt information epinfo
   Input image and assign it to image
   if run LSB algorithm success then
     Get encrypt image epima1
     Input MLNCML sequence and assign it to ms
     if run secondary algorithm success then
       Output last encrypted image lctima
       return lctima
     else prompt error information
       return
     end if
   else prompt error information
     return
   end if
else prompt error information
  return
end if
```

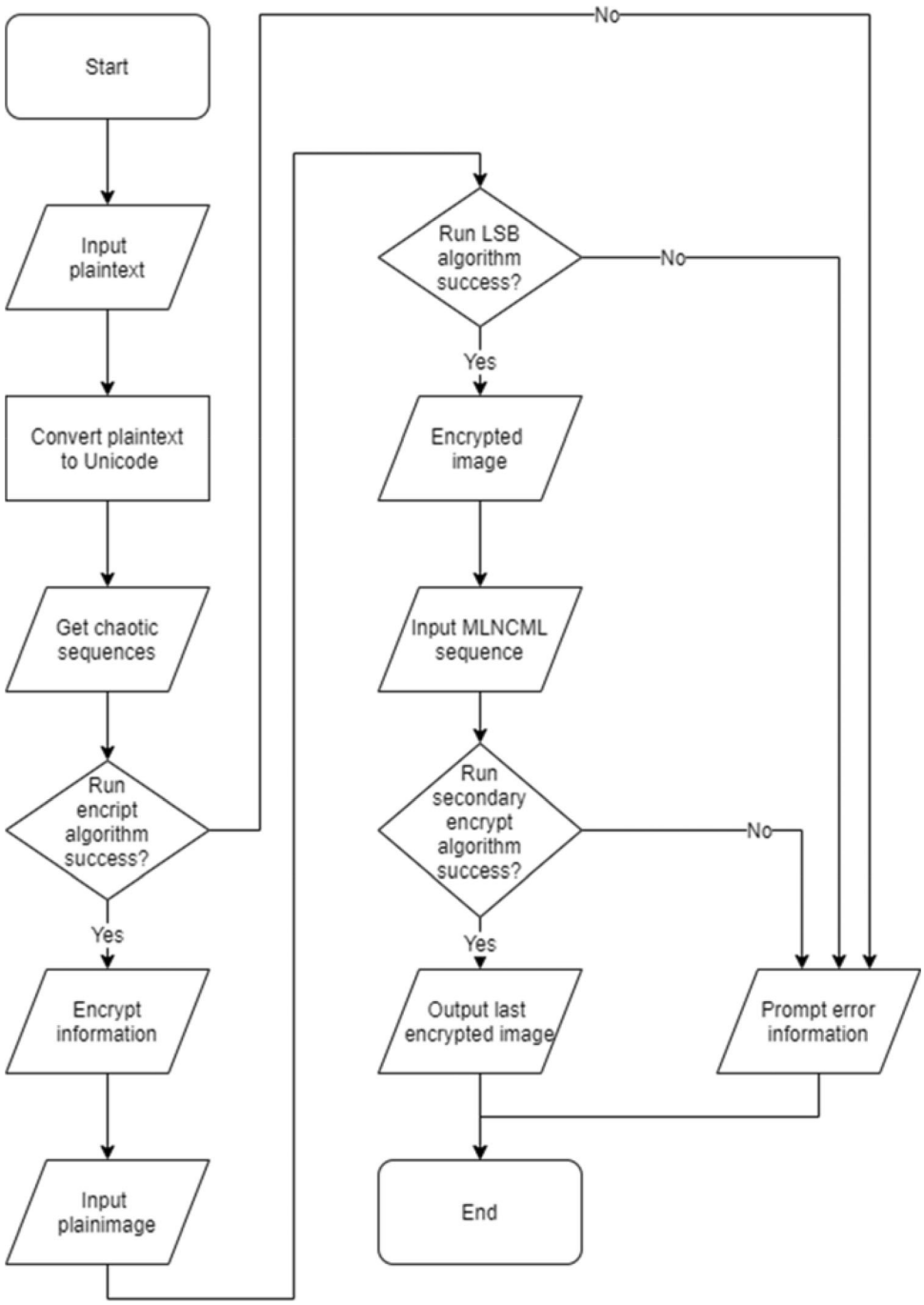


Fig. 5 LSB image encryption algorithm flowchart combined with MLNCML

A detailed blockchain-based access control model combined with chaotic encryption, LSB algorithm, ABAC access control is proposed. The conceptual model of the proposed method is shown in Fig. 6. The specific workflow of the access control model is as follows:

1. The IoT devices generate data and upload data to edge nodes.
2. The edge node generates corresponding access control attributes and corresponding model control strategies for a specific resource and uploads them to the blockchain. It also generates the corresponding chaotic sequences and MLNCML sequences and uploads them to the chaotic sequence coding library.
3. The edge node uses the chaotic sequence and MLNCML sequence to hide and encrypt the IoT data using the appropriate carrier map and uploads the encrypted secret map to the cloud storage.
4. The resource requester sends a resource access request to the policy enforcement point (PEP).

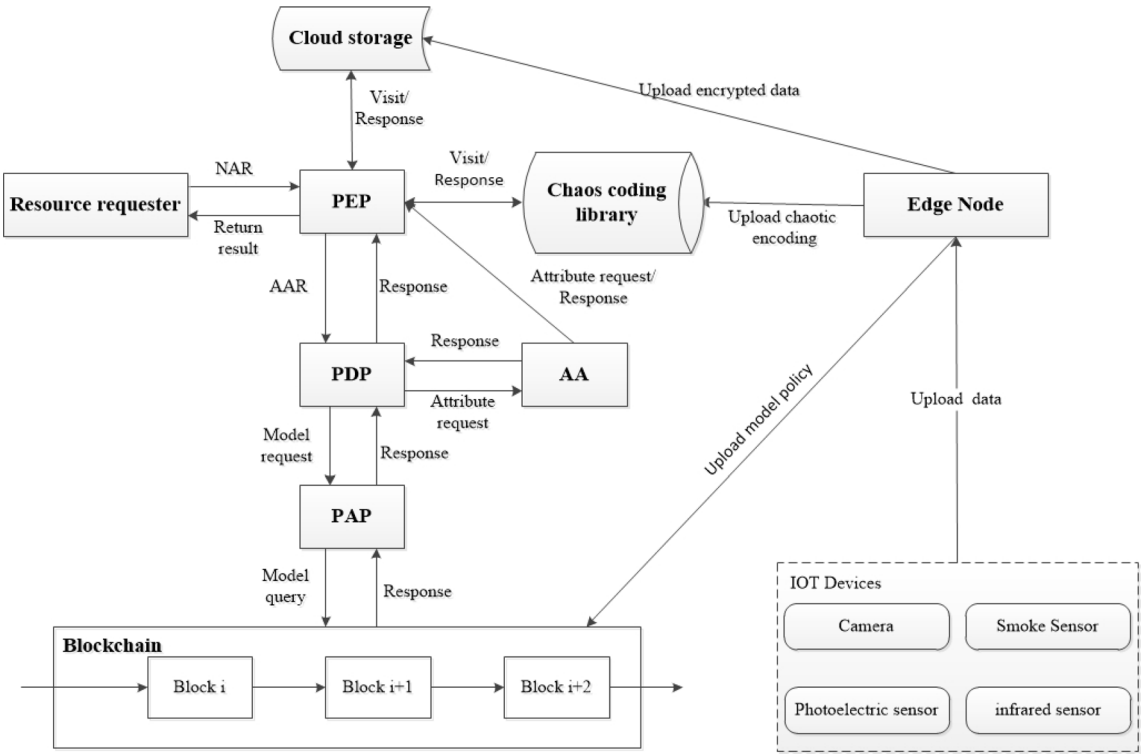


Fig. 6 Blockchain-based access control model

5. The PEP then constructs the AAR according to the access request and attributes information and sends it to the policy decision point (PDP).
6. The PDP requests to the PAP to query the access control policy related to the subject of the resource requester.
7. PAP inquires the relevant policies of the resource side in the Blockchain according to the AAR.
8. Then PAP feeds back the query results from the blockchain to the PDP;
9. The PDP makes a decision based on the resource side policy, resource requester's attribute information, and current environmental attributes, etc., and obtains the decision results such as allowed or denied access and feeds it back to the PEP.
10. PEP is executed according to the judgment result fed back by the PDP. If it is allowed, according to the information of the resource requester, it looks for the corresponding chaotic sequence and MLNCML sequence in the chaotic sequence coding library and returns these two sequences to the resource requester. After allowing the resource requests, the requester goes to the cloud storage to download the corresponding encrypted resource, and then the requester decrypts and recovers the plaintext information according to the chaotic sequence and MLNCML sequence for the acquired resource.

Note that throughout the whole process, the security of data is guaranteed by the encryption of chaotic sequence encoding. The acquisition of chaotic sequence encoding is obtained through dynamic access control, which saves the key distribution process. Besides, storing the access control model strategy on the alliance blockchain has two main advantages: (1) Only the participants of the alliance blockchain can access the strategic data on the blockchain, and the participants must get a license certification to join the blockchain, to increase the safety of system; (2) The strategic data on the alliance chain is distributed, which can prevent data from being tampered and can ensure the validity of the data.

In combination with Casbin, ABAC-based access control requires only the resource owner to define an access control models. It does not define any complex or numerous access policies. The resource owner can store the access control model strategy based on the Casbin definition on the blockchain, and it is open to all alliance blockchain members.

Since the resources that require access control are general resources with certain confidentiality requirements, i.e. certain requirements are for the subjects that can access the resources. At the same time, post-audit audits of the accessed users are required. After comprehensive consideration, alliance chain technology should be used for implementation. In addition, the model policy data on the block has a timestamp that is recognized by the entire alliance, which can provide

effective support for the timeliness of corporate access control and the fairness of post-event audits.

5 Experiments and evaluation

In this section, first, we will validate the proposed method by using a case study of IoT data sharing for smart city and then, provide a Security analysis of this method. At last, we provide a comparative analysis of the proposed method with the state-of-art mechanism included in this section.

5.1 Experimental setup

In this case study, the process of distributed access control and sensitive IoT data sharing is demonstrated. The algorithm for the distributed access control is programed by Go language and it can run in JetBrains developer tools. The encryption and decryption algorithm using Mixed Linear-Nonlinear Coupled Map Lattice and Least Significant Bit Method algorithm is programmed in MATLAB language and simulated in MATLAB developer tools.

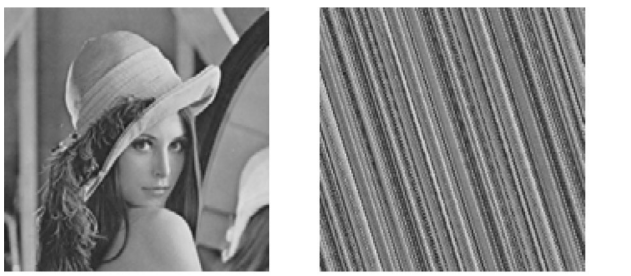
To provide the validation of the proposed mechanism, we use communication in a smart city as a case study due to its significance in IoT-based systems. A smart city system contains a lot of heterogeneous sensors from different IoT systems. Different users may use the data in their applications. Furthermore, some sensors in a smart city may generate sensitive data which should get secured by some means. The use of encryption is important in distributed systems, where some data is very confidential. If the data is not properly encrypted, the attacker can easily get the data which leads to serious consequences, even it can harm the smart city management. This paper proposes a security mechanism for securing the privacy of the data. The whole working process of the mechanism is described below.

1. The edge node generates the corresponding chaotic sequence and MLNCML sequence code through the chaos theory described above.
2. The edge node selects the lena.jpg picture as the carrier picture. The information that needs to be encrypted and hidden is as follows: “plaintext information”. Figures before and after encryptions are shown in Fig. 7.
3. The edge node uploads the encrypted map to the cloud storage platform.
4. The edge node uploads the corresponding chaotic sequence code to the chaotic code library.
5. The edge node generates the corresponding access control model policy, which contains the access control requirement referring to the IoT device. The access model strategy is as follows:

```
[request_definition]
r = sub, obj, act, env
[policy_definition]
p = sub, obj,act
[policy_effect]
e = some(where (p.eft == allow))
[matchers]
m = r.sub.Role=='Admin' && r.sub.Credit_score>=70&&r.obj.Name=='Cloud encode image
resource' && r.act in('read','copy') && r.env.Time.Hour >7 && r.env.Time.Hour <= 18
```

Note that the role of the resource requester must be the administrator of the enterprise. The enterprise credit score is 70 or more and the IoT devices can be accessed only at 7 am and 6 pm. After the model strategy is created, it is automatically uploaded to the blockchain.

6. When the resource requester A needs to access the IoT device, it sends an access request to the PEP at 10 am, the request contains the relevant attribute information of the resource requester, where Role = ’Admin’, and Credit_score = 90.



(a) Plain image (b) Encrypted image

Fig. 7 Plain image and Encrypted image

Table 1 Results of changing the value of parameter μ

Chaos coding parameter μ	Decryption result	Bit error rate
3.75	Plaintext information	0
3.76	Index out of bounds error	100%
3.74	Index out of bounds error	100%

Table 2 Results of changing the value of encrypted image pixels (1, 1)

Encrypted image pixels (1,1) value	Decryption result	Bit error rate
10011110	Plaintext information	0
10011111	Index out of bounds error	100%
10011101	Index out of bounds error	100%

7. The PEP constructs the AAR according to the access request and attributes information and sends it to the PDP.
8. The PDP inquires to the PAP to query the access control policy related to the requester's subject.
9. PAP inquires the relevant policies of the IoT device-side in the Blockchain according to the AAR.
10. PAP feeds back the query results from the blockchain to the PDP.
11. The PDP makes a judgment based on the IoT device-side policy, resource requester's attribute information, and the current environmental attributes (env.Time.Hour = 10). The judgment results are as follows:

    Time: 2020-02-20 10:00:00 +0800 CST

    Admin read record: true

    This is the result of the access decision and is then sent as feedback to PEP.
12. PEP executes according to the judgment result fed back by the PDP. It searches for the corresponding chaotic and MLNCML sequence code in the chaotic sequence coding library according to the information of the resource requester and returns the two sequences to the resource requester while allowing the resource requester to access the cloud storage to download the corresponding encrypted IoT data. The resource requester then decrypts and recovers the plaintext information according to the chaotic and MLNCML sequence. The recovered information is: "plaintext information";

13 The entire process ends.

Note that in the whole process, the PDP is responsible for the decision of the dynamic access control request, while the PEP is responsible for the implementation of the access control. If the decision given by the PDP is to allow access, the corresponding chaotic coding and the address of the resource in the cloud storage will be returned to the resource requester. Otherwise, the denial of access is the result of the resource requester.

To verify the anti-attack ability of the encryption scheme proposed in this paper, the following two experimental schemes were designed:

1. When the value of the core parameter μ in the chaotic coding is modified. The decryption results are shown in Table 1;
2. When the value of the first pixel of the encrypted image is modified, the original value is 10011110. The decryption results are shown in Table 2.

According to the above experimental results, it can be seen that the proposed encryption scheme is very sensitive to chaotic encoding parameters and encrypted data. Therefore, it can prevent modification attacks.

5.2 Security analysis

Security is the main objective of our work. We present here a detailed security analysis of the proposed framework including file storage security, anti-data tampering, data theft prevention and data privacy.

1. *File storage security* The file is encrypted before it is uploaded to the cloud. In the case where the chaos coding is not available, the file cannot be decrypted, that is, the attacker cannot view the plain data. In this way, all the stored data are safe.
2. *Anti-data tampering* All the files stored on cloud are encrypted. Suppose an attacker gets an encrypted file by some means and wants to tamper the contents of the file, with the help of chaos coding, it is very difficult to decrypt the files without obtaining a proper chaos code.
3. *Theft prevention* Suppose if the attacker attempts to replace the real file stored in the system with a fake file by applying some malicious methods, the replaced file will not be entertained because of hashing used in this technique. In this mechanism, when a resource owner uploads an encrypted file, a hash value will be calculated for the plain file, and this hash value is uploaded with the encrypted file. A repetitive hash

value check is required for a file after decryption. When the attacker intends to use a fake file F0, the hash obtained by the hash algorithm is hashF0. Whereas, the hash obtained by the hash algorithm for the source files F is hashF1. According to the hash rule, if the hash value obtained by hashing two files are not identical then the file is considered corrupt, that is, the file is replaced by an attacker. Therefore, our mechanism ensures that the user's source file cannot be replaced by the fake file used by the attacker, thereby ensuring the security of the user's data file.

4. *Data Privacy* The access control protocol allows the user to have absolute control over the data files. Firstly, the resource owner can make the access control model policy and store it in the blockchain. Secondly, the resource owner can dynamically update the access control model policy and achieves the fine-grained access control of resources. Only the authorized users who have relevant properties meeting the model policy requirements can get the access permission to obtain the encrypted files and get the chaos coding to decrypt the encrypted files. This way the resource requestor can only view the required data files without seeing other sensitive information, making the access control protocol is very secure.

The access control model policies are stored on the blockchain to secure them from being tampered with to achieve effective security of access control. At last, the Chaos model and LSB algorithm are introduced for the encryption of the data. This method has a huge key space and is very difficult to crack the key via brute force attacks. As a result, the privacy of data is well protected.

5.3 Comparative analysis

The use of blockchain technology combined with access control to protect privacy can also be used in medical information, IoT, and cloud data. The results of the comparison with the existing solutions are shown in Table 3.

Compared with MDSM [38] that uses the DPOS algorithm, the number of start-up nodes required is much less than MDSM. Furthermore, MDSM needs to set the voting rights and ratio in the final results for the users manually.

Compared with the BACC [39], our proposed mechanism provides dynamic access control as BACC uses the access control list (ACL) where the subjects (data users) and the permissions granted to them are defined by the data owner which can't be updated. Furthermore, the number of nodes required to maintain the blockchain system is much less than BACC in our technique and it is not required to pay when the information is submitted to the blockchain.

Compared with [40], the number of nodes required to maintain the blockchain system is far much less than that proposed in [40].

The authors in [41] implemented the octal permission representation to represent the access permissions granted to users, it does not support dynamic access control. The proposed blockchain-based system for data access control management uses Ethereum, thus, it needs to pay when using the Ethereum.

The authors in [42] proposed a blockchain-based privacy-preserving federated learning (BC-based PPFL) framework, which leverages the immutability and decentralized trust properties of blockchain to provide provenance of model updates. In that solution, the server generates a pair of public and private keys for each task which means it does not support dynamic access control. The blockchain is built over Ethereum and chain operations are controlled using the Truffle suite, which is a development and testing framework for Ethereum, thus it needs to pay when using the Ethereum.

The authors in [18] proposed a smart IoT system by using the Ethererum based blockchain system. But it does not support dynamic access control. The blockchain is built over Ethereum, so it needs a lot of nodes, and need to pay when using the Ethereum.

After comparing the literature cited above, it can be seen that the proposed blockchain system does not need to pay remuneration, requires a fewer start-up and running nodes which can be extended later. It requires less computing power and does not need to artificially set the proportion of voting rights. Moreover, the dynamic access control strategy can be formulated by using ABAC, and the effective

Table 3 Comparison of security performance

System	Dynamic access control	Number of nodes	Voting weight setting	Pay
MDSM [38]	No	121	Yes	No
BACC [39]	No	Many	No	Yes
Work in [40]	Yes	Many	No	No
Work in [41]	No	Many	No	Yes
Work in [42]	No	Many	No	Yes
Work in [18]	No	Many	No	Yes
Our work	Yes	Less, at least three	No	No

management of the rights can be realized. These are the unique features and advantages of the solution.

6 Conclusion and future work

This paper addressed the existing security problems related to IoT data privacy as a result of its vulnerability to data leakage. Moreover, the network, being used for data transfer, is not safe and brings privacy leakage issues. We proposed an access control model based on blockchain technology that embeds the relevant characteristics of blockchain technology, chaotic encryption technology, LSB technology, and ABAC, combined with the Casbin access control framework. Using the ABAC as access control technology, the edge node can assign the appropriate properties to the IoT data file, and only resource requesters with matching property requirements can access the IoT data file, setting the first barrier for protecting the IoT data file. Next, by using the hyperledger fabric blockchain technology, the file access model policies with timestamps are stored in blocks that are pre-defined by the edge node. At any particular time, an edge node can update the model policies by uploading a new model policy to the blockchain with a new timestamp giving the option of dynamic access controls. The PDP will use the latest model policy file to make an access control decision. Lastly, the IoT data is encrypted by chaotic and LSB technology, only the resource requester that meets the access control requirements can get the chaotic and MLNCML sequence code to decrypt the data.

We have also demonstrated how the IoT data sharing process between alliance chains can be adopted. We described the effectiveness of the framework in the resource access scenario of the cloud storage platform. The framework can solve the problem of a single point of failure of access control by using the alliance chain node as PDP. Each PDP node has the whole access control policy ledger. If one alliance chain node is down, another node can be used as a new PDP node. We also discussed the effectiveness of the model through experiments, a security analysis, and comparative analysis with the related work. It has been verified that t the proposed framework can achieve fine-grained access control based on blockchain technology for sensitive data between alliance nodes.

To make the system more practical, the first future work would focus on the development of a lightweight consensus protocol, which has good performance in throughput and quick confirmation. Another very fruitful research area is the application of blockchain technology to use smart contracts to implement distributed access control system in IoT, which can make the access control more effective and avoid single points of failure. The third interesting direction is to use trusted computing technology to ensure the credibility and security of edge nodes.

Acknowledgements I would like to express my heartfelt gratitude to Dr. Vivek Nallur, an assistant professor who works in Computer Science, University College Dublin. He provided great help during the preparation of the manuscript.

Funding This research was sponsored by the International Research Cooperation Seed Fund of Beijing University of Technology (No. 2018A01).

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

Compliance with ethical standards

Conflict of interest The authors declare that there is no conflict of interest regarding the publication of this paper.

References

1. Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K.: A survey on the internet of things (IoT) forensics: challenges, approaches and open issues. IEEE Commun. Surv. Tutor. (2020). https://doi.org/10.1109/comst.2019.2962586
2. Abbas, N., Asim, M., Tariq, N., Baker, T., Abbas, S.: A mechanism for securing IoT-enabled applications at the fog layer. J. Sens. Actuator Netw. **8**(1), 16 (2019)
3. By, G.S.: More Than Half of Major New Business Processes and Systems Will Incorporate Some Element of the Internet of Things. Publicado em Janeiro (2016)
4. Miloslavskaya, N., Tolstoy, A.: Internet of Things: information security challenges and solutions. Clust. Comput. **22**(1), 103–119 (2019)
5. Pavithran, D., Shaalan, K., Al-Karaki, J.N., Gawanmeh, A.: Towards building a blockchain framework for IoT. Clust. Comput. **2020**, 1–15 (2020)
6. Gatouillat, A., Badr, Y., Massot, B., Sejdić, E.: Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine. IEEE Internet Things J. **5**(5), 3810–3822 (2018)
7. Khalid, U., Asim, M., Baker, T., Hung, P.C., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Clust. Comput. **2020**, 1–21 (2020)
8. Pal, S., Rabehaja, T., Hill, A., Hitchens, M., Varadharajan, V.: On the integration of blockchain to the internet of things for enabling

access right delegation. IEEE Internet Things J. **7**(4), 2630–2639 (2019)
9. Xia, Q., Sifah, E.B., Agyekum, K.O.-B.O., Xia, H., Acheampong, K.N., Smahi, A., Gao, J., Du, X., Guizani, M.: Secured fine-grained selective access to outsourced cloud data in IoT environments. IEEE Internet Things J. **6**(6), 10749–10762 (2019)
10. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (IoT) security: current status, challenges and prospective measures. In: Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341. IEEE (2015)
11. Hammi, M.T., Hammi, B., Bellot, P., Serhrouchni, A.: Bubbles of Trust: a decentralized blockchain-based authentication system for IoT. Comput. Secur. **78**, 126–142 (2018)
12. Ali, M.S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., Rehmani, M.H.: Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun. Surv. Tutor. **21**(2), 1676–1717 (2018)
13. Li, D., Cai, Z., Deng, L., Yao, X., Wang, H.H.: Information security model of block chain based on intrusion sensing in the IoT environment. Clust. Comput. **22**(1), 451–468 (2019)
14. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., Jararweh, Y.: Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Clust. Comput. **2020**, 1–15 (2020)
15. Li, H., Pei, L., Liao, D., Wang, X., Xu, D., Sun, J.: BDDT: use blockchain to facilitate IoT data transactions. Clust Comput. (2020)
16. Ma, M., Shi, G., Li, F.: Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario. IEEE Access **7**, 34045–34059 (2019)
17. Alfandi, O., Otoum, S., Jararweh, Y.: Blockchain solution for IoT-based critical infrastructures: byzantine fault tolerance. In: Proceedings of the NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1–4. IEEE (2020)
18. Mohanta, B.K., Jena, D., Ramasubbareddy, S., Daneshmand, M., Gandomi, A.H.: Addressing security and privacy issues of IoT using blockchain technology. IEEE Internet Things J. (2020)
19. Zhaofeng, M., Xiaochang, W., Jain, D.K., Khan, H., Hongmin, G., Zhen, W.: A blockchain-based trusted data management scheme in edge computing. IEEE Trans. Ind. Inf. **16**(3), 2013–2021 (2019)
20. Nakamoto, S., Bitcoin, A.: A peer-to-peer electronic cash system. Bitcoin.: https://bitcoin.org/bitcoin.pdf (2008)
21. Niranjanamurthy, M., Nithya, B., Jagannatha, S.: Analysis of blockchain technology: pros, cons and SWOT. Clust. Comput. **22**(6), 14743–14757 (2019)
22. Wedaj, F.T., Kim, S., Kim, H.J., Huang, F.: Improved reversible data hiding in JPEG images based on new coefficient selection strategy. EURASIP J. Image Video Process. **2017**(1), 63 (2017)
23. Weng, S., Zhang, G., Pan, J.-S., Zhou, Z.: Optimal PPVO-based reversible data hiding. J. Vis. Commun. Image Represent. **48**, 317–328 (2017)
24. Ke, Y., Zhang, M.-Q., Liu, J., Su, T.-T., Yang, X.-Y.: A multi-level reversible data hiding scheme in encrypted domain based on LWE. J. Vis. Commun. Image Represent. **54**, 133–144 (2018)
25. Zhu, K., Cheng, J.: Color image encryption via compressive sensing and chaotic systems. In: Proceedings of the MATEC Web of Conferences, p. 03017. EDP Sciences (2020)
26. Wang, X., Guan, N., Zhao, H., Wang, S., Zhang, Y.: A new image encryption scheme based on coupling map lattices with mixed multi-chaos. Sci. Rep. **10**(1), 1–15 (2020)
27. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Process. **147**, 133–145 (2018)
28. Batista, C.A., Viana, R.L.: Quantifying coherence of chimera states in coupled chaotic systems. Phys. A **526**, 120869 (2019)
29. Yadav, G.S., Ojha, A.: Secure data hiding scheme using shape generation algorithm: a key based approach. Multimed. Tools Appl. **77**(13), 16319–16345 (2018)
30. Hu, V.C., Ferraiolo, D., Kuhn, R., Friedman, A.R., Lang, A.J., Cogdell, M.M., Schnitzer, A., Sandlin, K., Miller, R., Scarfone, K.: Guide to attribute based access control (abac) definition and considerations (draft). NIST Spec. Publ. **800**, 162 (2013)
31. Kanwal, T., Anjum, A., Khan, A.: Privacy preservation in e-health cloud: taxonomy, privacy requirements, feasibility analysis, and opportunities. Clust. Comput. **2020**, 1–25 (2020)
32. Banerjee, S., Roy, S., Odelu, V., Das, A.K., Chattopadhyay, S., Rodrigues, J.J., Park, Y.: Multi-Authority CP-ABE-Based user access control scheme with constant-size key and ciphertext for IoT deployment. J. Inf. Secur. Appl. **53**, 102503 (2020)
33. Ali, S., Wang, G., White, B., Cottrell, R.L.: A blockchain-based decentralized data storage and access framework for pinger. In: Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1303–1308. IEEE (2018)
34. Novo, O.: Blockchain meets IoT: an architecture for scalable access management in IoT. IEEE Internet Things J. **5**(2), 1184–1195 (2018)
35. Fan, S., Song, L., Sang, C.: Research on privacy protection in IoT system based on blockchain. In: Proceedings of the International Conference on Smart Blockchain, pp. 1–10. Springer (2019)
36. Ghadekar, P., Doke, N., Kaneri, S., Jha, V.: Secure access control to IoT devices using blockchain. Int. J. Recent Technol. Eng. **8**(2), 3064–3070 (2019). https://doi.org/10.35940/ijrteF2273.078219
37. Nakamura, Y., Zhang, Y., Sasabe, M., Kasahara, S.: Exploiting smart contracts for capability-based access control in the Internet of Things. Sensors **20**(6), 1793 (2020)
38. Xue, T.F., Fu, Q.C., Wang, C., Wang, X.Y.: A medical data sharing model via blockchain. Zidonghua Xuebao/Acta Automatica Sinica **43**(9), 1555–1562 (2017). https://doi.org/10.16383/j.aas.2017.c160661
39. Sohrabi, N., Yi, X., Tari, Z., Khalil, I.: BACC: blockchain-based access control for cloud data. In: Proceedings of the Australasian Computer Science Week Multiconference, pp. 1–10 (2020)
40. Tang, B., Kang, H., Fan, J., Li, Q., Sandhu, R.: Iot passport: a blockchain-based trust framework for collaborative internet-of-things. In: Proceedings of the 24th ACM Symposium on Access Control Models and Technologies, pp. 83–92 (2019)
41. Samaniego, M., Espana, C., Deters, R.: Access control management for plant phenotyping using integrated blockchain. In: Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, pp. 39–46 (2019)
42. Awan, S., Li, F., Luo, B., Liu, M.: Poster: A reliable and accountable privacy-preserving federated learning framework using the blockchain. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 2561–2563 (2019)

Yanhui Liu received his B.S. degree in computer science and technology from Northwest University in 2007, Xi'an, China and the M.S. degree in computer science and technology from Beijing University of Technology, Beijing, China, in 2010. He is currently pursuing the Ph.D. degree in computer science and technology in Beijing University of Technology, Beijing, China. His research interests include cloud security, Blockchain technology, information security, and trusted computing.

Jianbiao Zhang , was born in 1969. He received the B.S., M.S. and Ph.D. degrees from the Northwestern Polytechnic University, Xi'an, Shanxi, in 1992, 1995 and 1999, respectively. From 1999 to 2001, he was a postdoctoral fellow in BeiHang University, Beijing. Now, he is a professor and Ph.D. supervisor in Faculty of Information Technology, Beijing University of Technology. His research interests include trusted computing, system security, cloud security and blockchain. He has published over 80 journal/conference papers.

Jing Zhan , an Assistant Professor at College of Computer Science, Beijing University of Technology, China. She received her Ph. D. degree from Wuhan University in 2009. Her current research interests lie on the areas of cloud security and trusted computing, particularly design and implementation of secure cloud services.