IET Communications

Research Article

Research on distributed blockchain-based privacy-preserving and data security framework in IoT

ISSN 1751-8628
Received on 28th May 2019
Revised 25th January 2020
Accepted on 18th February 2020
E-First on 29th May 2020
doi: 10.1049/iet-com.2019.0485
www.ietdl.org

Hongliang Tian[1,2] ✉, Xiaonan Ge[1,2], Jiayue Wang[1,2], Chenxi Li[1,2], Hongle Pan[1,2]

[1]Key Laboratory of Modern Power System Simulation and Control & Renewable Energy Technology, Ministry of Education, Northeast Electric Power University, Jilin, People's Republic of China
[2]School of Electrical Engineering, Northeast Electric Power University, Jilin, People's Republic of China
✉ E-mail: hltian@foxmail.com

Abstract: With the rapid development of the Internet of things (IoT), it has brought great convenience for people's life. However, the security and privacy of IoT still face a major challenge. To remedy these issues, in this study, the authors first introduce the three-tier architecture of IoT and analyse the corresponding security problems of each layer, then they discussed the compatibility between IoT and blockchain. Secondly, they propose a new, distributed blockchain-based security architecture of IoT, which rely on gateway nodes of perception layer to secure data storage and sharing, and use middleware servers to analyse and process data. Finally, they adopt game theory to model and analyse their designed scheme. The results demonstrate that their scheme is a safe and deployable framework for IoT data security and privacy.

1 Introduction

At present, the connected devices scale of Internet of things (IoT) is growing exponentially, and the number of connected devices is predicted to reach anywhere from 20 to 50 billion by 2020 [1]. However, as more and more intelligent devices are connected to the network, the generated mass data is vulnerable to network attacks in the process of transmission and interaction, resulting in data modification or abuse, thus threatening the security of the entire IoT system. Moreover, due to a diverse integration of devices, network and services, the data stored on a device is vulnerable to privacy violation by compromising nodes existing in an IoT network [2]. As for privileged access to services between two communication parties, these IoT devices may interact information across domains, and the communication between them should be verifiable, while the cost of establishing credit is high when multi-agent collaboration, and due to the heterogeneity of infrastructures and environments which support IoT devices, the diversity of IoT authentication mechanisms may lead to communication barriers, and the large amount of heterogeneous data generated from this increase the attack surface. Furthermore, because the IoT system is composed of resource-constrained devices and the current access control system is centralised, it may be vulnerable to a single point of failure. Due to all these problems and vulnerabilities, IoT applications create the conditions for a variety of cyber threats, and IoT applications deployed worldwide are subject to a variety of security and privacy attacks. Among them, Mirai attacks were estimated to infect about 2.5 million devices connected to the Internet and launch distributed denial of service (DDoS) attacks [3]. Therefore, there is an urgent need for an open architecture that can not only meet the interoperability requirements between different systems and distributed resources, but also ensure the overall security of the system. Blockchain technology provides new ideas and solutions for big data management, trust, security, privacy and other issues faced by IoT. Blockchain integrates distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm and other technologies, it is suitable for building mutual trust between heterogeneous system. Blockchain uses distributed peer-to-peer structure to manage devices with limited access control, reduces the operation and credit cost of a centralised network, and is expected to solve the weakness of IoT security [4]. The technology is one of the most revolutionary emerging technologies in recent years, which not only has a big breakthrough in the financial field, but also has a very broad application scene in many fields such as electronic voting, certificate issuing agencies, IoT and other intelligent systems. It has been highly concerned by all walks of life, and the development of blockchain technology has become an irreversible trend.

The organisation of this paper is as follows. In Section 2, we review related work and discuss the benefit of our scheme. Section 3 introduces the demand analysis on the introduction of blockchain technology into IoT. Section 4 describes the technology architecture of the IoT based on blockchain. Section 5 presents the operation mechanism of the proposed architecture. Sections 6 and 7 analyse the security and performance of our scheme, respectively. Section 8 concludes the paper and describes future work.

2 Related work

In this section, we review the main previous related work about privacy-preserving and data security in IoT. We will describe the related work from the following two aspects and mainly focus on authentication, confidentiality, integrity, non-repudiation and privacy.

2.1 Traditional cryptographic approaches

To address the main IoT security services, there were many solutions based on cryptographic have been proposed. However, in most cases, these solutions are inefficient or even inapplicable in resource-constrained IoT devices, because these cryptographic algorithms are very greedy in terms of storage and computation [5], so we are only investigating a few lightweight cryptographic solutions in recent years.

In [6], the authors proposed a new fuzzy identity-based encryption (FIBE) scheme to ensure the security of IoT data, their proposed FIBE scheme eliminates the dependence on random oracle models and is secure in the full model. Tan *et al.* [7] presented the enhancement of a lightweight key-policy attribute-based encryption (KP-ABE) scheme for IoT. The authors extended the fixed KP-ABE into a hierarchical KP-ABE (H-KP-ABE) scheme which addresses the poor generality in the original scheme, the proposed H-KP-ABE scheme is suitable for IoT applications which perform encryption and role delegation on low powered devices but decryption on the server. Aghili *et al.* [8] proposed a new secure, energy-efficient protocol for e-health system that supports ownership transfer. The lightweight protocol not only provides authentication and key agreement but also satisfies access control and protects the privacy of doctors and patients. In [9], aiming at the IoT devices vulnerable to physical and cloning attacks, the authors presented a lightweight and privacy-preserving two-factor authentication scheme. The scheme utilised a password or a shared secret key as the first authentication factor and the physically unclonable functions as the second authentication factor, thus providing the desired security characteristics efficiently. Of course, there are many other similar solutions which we will not list them all here. Nevertheless, through comparative analysis, we found that some schemes may not be used on microcontrollers with small RAM memory, and may have a certain delay on devices with limited computation, which may not be applicable in applications with high real-time requirements. In addition, most traditional security approaches rely on a centralised architecture and therefore have a single point of failure. Moreover, with the geometric growth of IoT devices, the cost of centralised service is difficult to afford, and the third-party central server manager may use it to store and forward private data without authorisation, resulting in the disclosure of personal privacy. Therefore, a decentralised distributed architecture is needed to solve the security problem of IoT, and blockchain is seen as the best technology to solve these problems.

2.2 New blockchain approaches

As an independent technology, blockchain can be traced back to the bitcoin system, which is used to ensure that transaction records are true, valid and cannot be tampered with [10]. Blockchain is a distributed database that does not need a central authority or third-party verification. Once proposed, blockchain has become one of the most popular research topics and rapidly extended to many fields, such as supply chain, business, healthcare, IoT and data management.

Reyna *et al.* [11] investigated the blockchain technology, analysed its unique functions and open challenges, and discussed the potential application of the integration of blockchain and the IoT. Minoli and Occhiogrosso [12] summarised the present status of IoT security environment and various uses of blockchain in every layer of the IoT reference framework. It also briefly introduced some IoT environment where blockchain mechanism can play an important role, such as electronic health and vehicular traffic system, and pointed out that blockchain can be used as a security solution of IoT. Hammi *et al.* [13] proposed a distributed system called ‘bubbles of trust’, which is used to identify and verify IoT devices and ensure the integrity and availability of data. The authors used blockchain to create secure virtual zones for secure communication and mutual trust. He *et al*. [14] proposed a blockchain-based privacy protection management scheme for IoT devices, which combines attribute-based encryption with time-limited key management technology to achieve privacy protection and device management. Qian *et al*. [15] introduced the corresponding security problems of three layers in IoT and proposed a high-level security management scheme based on blockchain for different IoT devices in the full life cycle. With the interaction between IoT devices and blockchain database, the management solution adopts a device identification-based key algorithm to guarantee security and reliability. Dorri *et al.* [16] devised a theoretical lightweight architecture based on private blockchain in the context of a smart home, which reduces the communications overhead of workload proof mechanism by introducing the central miners. Yu *et al.* [17] investigated typical security and privacy issues in IoT and developed a framework to integrate blockchain with IoT, which can provide great assurance for IoT data and reliable scalability including authentication, decentralised payment, and so on. In [18], the authors analysed the applicability of blockchain to IoT devices and data management with an aim of providing end-to-end security for trading. The authors pointed out that blockchain as a distributed system is an ideal solution to the trust problem in IoT ecosystem, thus eliminating the worry about the security and privacy issues of the deployment of IoT data transaction platform. Angin *et al.* [19] proposed a data security architecture based on blockchain technology that introduces transparency and tamper-resistance into data storage and retrieval in IoT networks. The solution takes the resource constraints of IoT devices and the heterogeneity of IoT networks into consideration, which enables utilisation of powerful cloud servers for mining in the blockchain network. The presented system maintained the security and privacy of blockchain by relying on hierarchical structure and distributed trust. Many works and surveys discuss the security and privacy in IoT, however, only few of them analysed the compatibility between blockchain technology and IoT from the three-layer architecture, and the majority of the related works are in a theoretical verification stage, where only the description of the approach is provided and no implementations or simulations were realised. We first start from the issues faced by IoT and use blockchain to provide security and privacy, we proposed a general new security architecture by making full use of the storage capacity of gateway devices and computing resources of middleware.

In this paper, we present a new architecture for securing data and managing IoT devices. The architecture provides trust, ownership record, transparency and communication support for large-scale IoT. We adopt gateway devices to store data and build a P2P network for achieving information interaction. At the same time, the middleware server is used to process data and realise access control management. By adopting blockchain, it provides effective security and privacy protection for IoT.

Compared with other architectures that have been proposed to address data security and privacy of IoT, our scheme has the following advantages:

(1) *Trust and transparency:* All data are encrypted and stored in gateway nodes, and can only be used by specific entities after verification. In addition, all devices need to be registered before joining the network, so only legitimate devices can participate in the network. Data stored by gateway nodes in blockchain are visible to all peers.

(2) *Ownership record:* The original sensor data are encrypted and uploaded to the corresponding regional gateway node. Only middleware servers with the corresponding authority can trigger transaction and realise data access. Moreover, access records will be uploaded to cloud to form a distributed ledger that stores complete historical transaction records, providing traceability audit history record for the ownership of each device in the system.

(3) *Communication support:* In some different application scenarios, IoT terminal devices are different from each other, and communication protocols are also different. Inconsistencies of various standards lead to waste of resources and communication barriers between different kinds of heterogeneous devices. Our proposed architecture adopts hash algorithm to process data through integration, cleaning, conversion and other measures, to eliminate the multi-source heterogeneity of IoT data, and truly realise the interconnection of devices.

3 Demand analysis on the introduction of blockchain technology into IoT

In this section, we introduced the IoT reference framework and discussed the corresponding security problems of three layers, then analysed and compared the advantages of introducing blockchain in IoT. Finally, we summarised the advantages of Hyperledger-Fabric over other blockchain technologies.

3.1 IoT architecture and security problems

Nowadays, the generally accepted IoT architecture is divided into three layers: perception layer, network layer and application layer, as shown in Fig. 1. The three layers use different techniques to achieve different functions. Among them, the perception layer mainly realises how to recognise the existence of the object itself, locate the position and the movement of the object etc. Object recognition and information collection are the basic data sources for IoT application. However, due to the different perception and recognition technologies used in the information collection process, and the relatively independent collection process, the collected information types and data formats are diverse. Security threats such as node capture, malicious code injection attack and false data injection attack may be encountered in the perception layer [20].

The main function of the network layer is to use the existing network communication technology to realise fast, safe and reliable two-way transmission of perception data. The information transmission in the network layer is the key for the application layer to realise the specific application. However, due to various communication modes and complex transmission protocols, so the integration and collaborative operation of various heterogeneous data need to be considered. The network layer is vulnerable to security threats such as access attacks, DDoS/DoS attacks and data transmission attacks [20].

The application layer includes two parts: application support sub-layer and specific IoT application. It mainly integrates relevant content services according to the different application scenarios, and uses the perception information to realise intelligent management, application and service, such as intelligent transportation, smart city and telemedicine. Under the complex network environment, the application layer is easy to become the target of network attackers. The application layer can encounter issues such as data thefts, access control attacks, and sniffing attacks [20].

3.2 Integration analysis of blockchain technology and IoT

Blockchain is a distributed system with a traceable history, non-tampering and solving the problem of multi-party mutual trust. Through encryption authentication, authorisation and other mechanisms, the security and privacy of large-scale IoT can be guaranteed from storage, information transmission and other aspects, so blockchain effectively solves the industry pain points in the development of IoT. To ensure the authenticity of the obtained information, we can trace the record source through blockchain to ensure authenticity and effectiveness. When data are transmitted in the network, blockchain can be used to connect different protocols and devices, and provide the ability to manage query and analyse data in the P2P network, so as to realise the multi-network integration and the intelligent network processing. To realise the seamless connection between blockchain technology and IoT, the compatibility between the mentioned above should be demonstrated first. The benefits of blockchain integration with IoT are shown in Table 1.

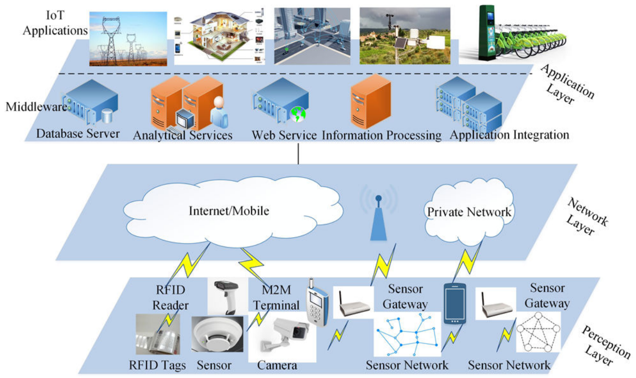

Fig. 1 *Reference architecture of the IoT*

3.3 Selection of blockchain technology in IoT

According to the access mechanism, blockchain technology can be divided into three categories: Public blockchain, Consortium blockchain and Private blockchain. The public blockchain is open to the public, users can anonymously participate in the system, generate transaction and reach consensus; Access and read–write rights are strictly controlled in the private blockchain; Alliance blockchain is a kind of blockchain requiring registration and licensing, which is only limited to the participation of alliance members. The read, write and participate in accounting rights can be formulated by alliance rules. The network of alliance blockchain is jointly maintained by member institutions, which is generally applicable to business-to-business scenarios such as transactions and settlement between institutions.

Hyperledger-Fabric [21] project based on Practical Byzantine Fault Tolerance (PBFT) [22] consensus protocol is a kind of alliance blockchain architecture, which can confirm information with low delay, energy consumption and computing cost without block bifurcation when multiple applications are deployed in the IoT system. In terms of resource consumption, IoT system such as sensors running in the smart city environment generate millions of information every day. Therefore, IoT platforms based on blockchain technology should not have transaction fee, while IoT architectures based on Hyperledger-Fabric can choose to set up information verification without charging fees [23]. In terms of consensus, consensus protocol based on PBFT has low energy consumption and can achieve rapid information authentication.

Moreover, PBFT supports consensus termination, that is once the data information is unanimously confirmed by most gateway nodes, written into the block and linked to the longest main blockchain, according to the PBFT protocol, the transaction will be considered to have been completed, to avoid malicious gateway nodes withdrawing the data information privately and threatening the normal operation of the IoT system; When managing IoT devices, smart contract can be deployed on Hyperledger-Fabric to perform automatic access control; In terms of privacy security, the IoT system needs to ensure the confidentiality of data when sharing data information, while only Hyperledger-Fabric can ensure data

Table 1 Compatibility analysis of blockchain and IoT platform

Feature	IoT	Blockchain + IoT
communication security	The lack of a unified language for IoT platform is likely to hinder the communication between multiple IoT devices, and the botnet of things created by Mirai, DDoS attacks and so on can cause equipment fault.	The verification and consensus mechanism of blockchain help prevent illegal or even malicious nodes from accessing the IoT. Data corruption of any one node will not affect the normal operation of other nodes.
multi-agent collaboration	Most IoT systems are multiorganisation networks within operators and enterprises, involving multiple operators. When multiple peer entities cooperate, the cost of establishing credit is relatively high.	The distributed P2P structure of blockchain, open and transparent algorithms can build mutual trust at a low cost, break the information silos, and promote multi-party collaboration.
individual privacy	In the heterogeneous IoT, when the information is transmitted across domains, it may cause the risk of personal privacy disclosure, and the third-party central server may use and forward its stored private data without authorisation.	All data in the blockchain are strictly encrypted, and the transmitted data is converted into corresponding ciphertext. Without the secret key, the plaintext cannot be obtained, so as to ensure the privacy of the data.
architecture	Most IoT platforms adopt the centralised management, with the rapid growth of access devices, the cost of managing and maintaining an IoT platform is huge, and the centralised architecture is vulnerable to a single point of failure.	Blockchain adopts distributed peer-to-peer network, all nodes in the network are in the same status, and there is no special central node and hierarchy structure. Moreover, blockchain does not need centralised servers, so avoid the expensive operation and maintenance costs.

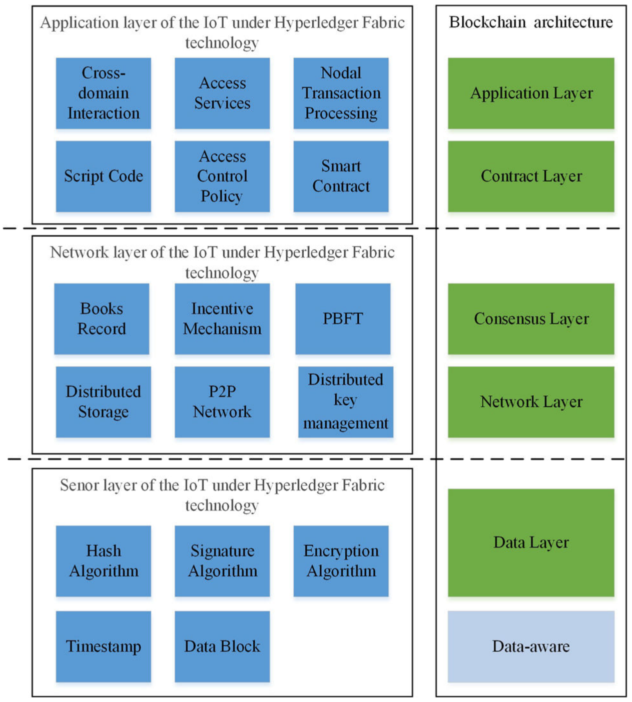

Fig. 2 *IoT security architecture based on blockchain*

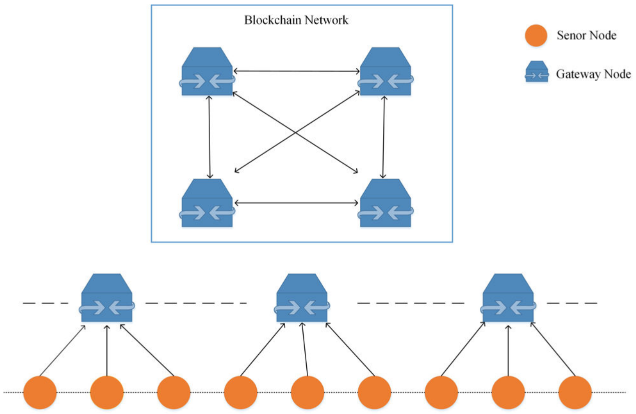

Fig. 3 *Distributed storage architecture of IoT under Hyperledger-Fabric technology*

privacy by creating dedicated channels and encrypting the data on the chain. Hyperledger-Fabric supports ID management and transaction authorisation of intelligent devices through public keys. As for performance, Hyperledger-Fabric has higher transaction throughput than bitcoin blockchain, Ethereum and so on [24]. From the above aspects, we can see that the Hyperledger-Fabric project based on PBFT is more suitable for IoT system.

4 IoT security architecture based on blockchain

In the perspective of Hyperledger-Fabric, the IoT security architecture can be divided into five levels: data perception layer, network transmission layer, consensus layer, contract layer and application layer. Each layer works together to form the basic architecture of IoT. The IoT security architecture based on blockchain is shown in Fig. 2.

4.1 Perception layer of IoT

The perception layer is the physical area and the basic module of IoT. Its main function is to identify objects, collect information and measure a variety of physical properties, such as temperature, humidity, air pressure and light. After the information is collected and extracted, the key information of different types of data is extracted through a specific hash function, asymmetric encryption, Merkle tree and other technical elements, and converted into fixed-length mathematical base to eliminate the heterogeneity of data. After the sensor data format is unified, the collected information is encapsulated into blocks, which is stored in the blockchain with a time-stamp and asymmetric encryption technology, and linked to the longest main blockchain to form a new block node.

(1) Signature encryption means that when the sensing data information is transmitted to a specific client application, the sender uses the public key of the receiver to carry out asymmetric encryption and sends the ciphertext to the receiver. After decoding the ciphertext into plaintext through the private key, the receiver can use the data information to realise various application services. Without the private key, the sensor data in the block cannot be decrypted into plaintext, which ensures that the sensor data will not be misappropriated by malicious users, thereby leading to the problem of privacy disclosure.

(2) The authentication process is as follows: when intelligent devices are registered into the system, the servers check whether the application has the corresponding access control rights according to the access control policy pre-defined in the smart contract, and the system verifies the ID information and IP address of the requested devices through the registration information stored in the blockchain. After verification, the system can log in for network management and intelligent services.

When the time-stamped sensor data is packaged into blocks, the corresponding gateway node will get the bookkeeping rights. The time-stamp is usually a sequence of characters, whose contents record important information such as the source of sensor data, digital signature and issuance time, which makes the sensor data highly traceable and ensures the high security of the blockchain network.

4.2 Network layer of IoT

The network layer contains the block network mode and data authentication protocol and other technical elements, so it can ensure that all block nodes in the whole network can participate in the transmission and ensure the reliability of data. In the network layer, each node has equal status and interacts with each other in a flat topology structure. Each node not only undertakes sensing data transmission, but also undertakes block information authentication, and also carries out network routing protocol.

From the structure of network layer, the IoT platform based on blockchain is a typical big data processing platform with decentralised and distributed storage. The advantage of this mode is that any node can authenticate, analyse and store sensor data without relying on the central servers. If the number of invalid nodes or illegal nodes $f < (n-1)/3(n$ is the total number of nodes), it will not affect storage and update of the main blockchain. The distributed IoT architecture based on Hyperledger-Fabric technology is shown in Fig. 3.

Various sensing devices upload all kinds of collected data to the blockchain and broadcast to the whole network nodes through the P2P network. When other nodes link to the new block information, the authenticity and validity of sensing data will be verified according to the data structure, key instruction, address source, time-stamp and other information. If the sensor data is true and reliable, the block node will store the sensing data in the block body according to the time series and continue to forward to the adjacent nodes. If the block receives illegal sensor data, the blockchain network will immediately stop the data transmission to ensure that the illegal data will not be forwarded in the IoT network. From the design of the network layer, it can be seen that the storage mode of distributed block nodes is highly tamper-proof, which ensures the security of the whole IoT system.

4.3 Consensus layer of IoT

Hyperledger-Fabric technology fundamentally solves the problem of block consensus and trust, enabling some distributed nodes to quickly reach consensus on different types of sensor data. The consensus layer adopts the PBFT consensus mechanism, which can

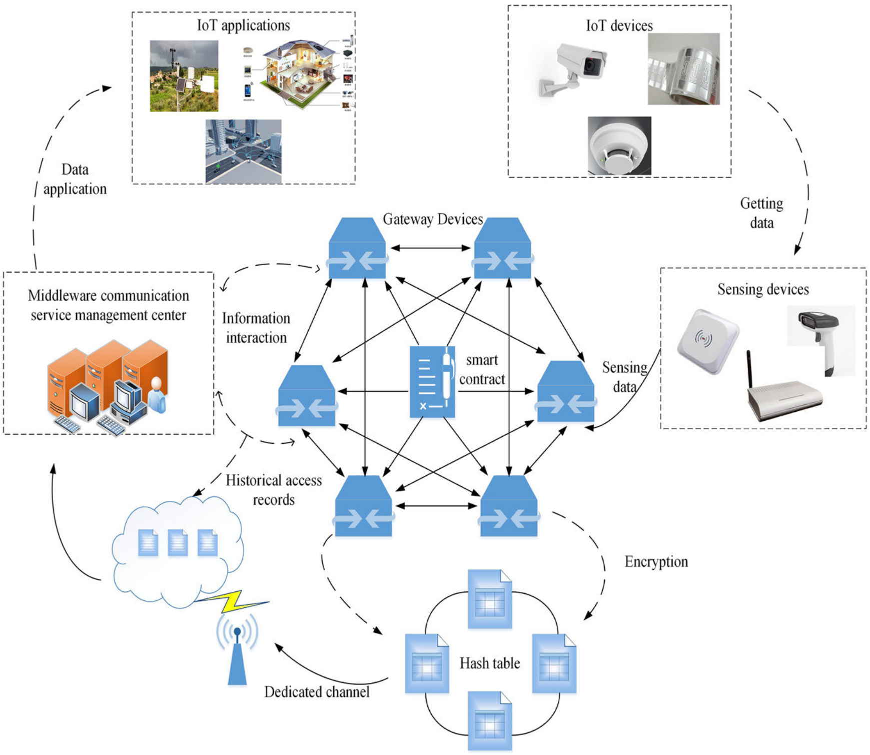

Fig. 4 *Application of Hyperledger Fabric in IoT*

achieve rapid authentication, reach nodes consensus, and ensure the data cannot be fabricated.

The PBFT consensus mechanism has lower computing cost and energy consumption, so it can achieve data authentication with the least energy and computing resources in the resource-limited IoT system. In the near real-time IoT environment, the adoption of PBFT can avoid the bifurcation of blockchain, thus leading to the delay of transaction confirmation. In addition, PBFT has a good fault tolerance, which can accommodate nearly one-third errors of the perceived nodes, as long as more than two-third of the nodes participate in the authentication, the IoT platform can operate normally.

4.4 Contract layer of IoT

The contract layer encapsulates various incentive mechanisms, script code, and the combination of more complex smart contracts. The smart contract is deployed in certificate authority as a stateless, event-driven and complete automatic execution code supporting Turing. After the event information is passed into the smart contract, the state machine is triggered for judgment. According to the pre-set information, if one or more of the actions meet the trigger condition, the state machine selects the corresponding access control policy to execute automatically.

In a large-scale heterogeneous IoT environment like Industry 4.0, the certificate authorities of each community manage their smart contracts, and the certificate authority in each region are interconnected to form an internal distributed network, which is finally connected to the large backbone network to access other domains. Through chain–chain architecture, interoperability in heterogeneous domains can also be achieved while implementing smart contracts for different scenarios to serve different needs.

The smart contract can effectively process the information, and ensure that counterparties can perform the contract compulsively without introducing a third party, so as to avoid the occurrence of default.

4.5 Application layer of IoT

The application layer encapsulates various application services, which provides efficient and reliable aggregation, calculation and processing for various data information, and realises the intelligent application of IoT.

The application layer includes two parts: the application support sub-layer and the specific application. IoT applications support the sub-layer to dynamically collect, store, decrypt, analyse and verify the encrypted data blocks.

For parts of the IoT work area where nodes deal with a large number of transactions, we can use the distributed characteristics of blockchain to make full use of idle nodes distributed in other different locations, where the nodes have certain computing power, storage capacity and bandwidth. The IoT application terminal reads the data information through the interface provided by the blockchain network, establishes the node transaction processing and access service in the process, and completes the information interaction between the middleware servers.

For example, after the gateway nodes hash the data, the corresponding hash table is encrypted and stored in the block. However, different gateway nodes belong to different middleware server management, when middleware servers need to access the data from other domains, it needs to determine whether it has the corresponding access control authority by triggering the smart contract. If so, the required data will be read from the distributed gateway nodes; if not, the request will be rejected. At the same time, through the state information of the devices, the application layer can judge whether there are problems of IoT devices in the operation process, to find and locate the faulty device's position in time, thus troubleshooting the faults and making the IoT platform run normally. Fig. 4 clearly shows the application process of Hyperledger-Fabric in IoT.

5 Operation mechanism of the proposed architecture

This section gives the operation mechanism of IoT under Hyperledger-Fabric technology, which consists of the data encryption and consensus, data decryption and application. In addition, due to the different division of labour nodes, here we adopt the hybrid network structure, that is we adopt a flat network structure between device and device, gateway and gateway, and we adopt hierarchical network structure between device and gateway, gateway and middleware. The communication protocol is cellular communications between gateway and gateway, gateway and middleware. Furthermore, between devices and devices, devices and gateways, they communicate with each other via Wi-Fi. The

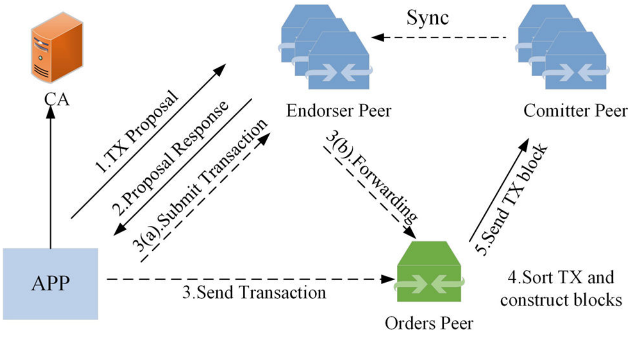

Fig. 5 *Interaction process of our proposed scheme*

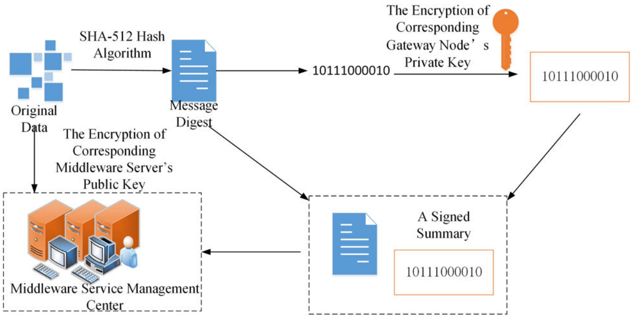

Fig. 6 *Data encryption and transmission process of IoT*

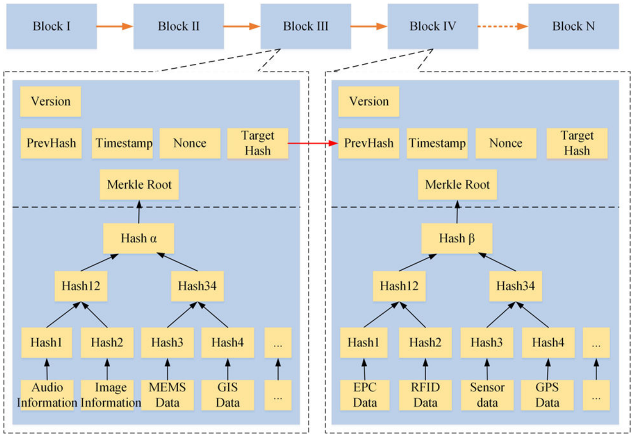

Fig. 7 *Structure of data block*

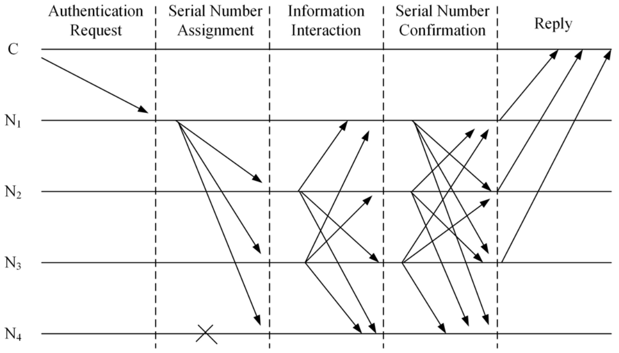

Fig. 8 *Consensus process of data block*

working mechanism of the proposed framework is presented as follows.

5.1 Data encryption and consensus of IoT

The information collected by IoT usually contains some important confidential and private information. To ensure the safe and reliable transmission of IoT data, the devices' identities need to be verified and the collected data need to be encrypted. In this phase, the whole specific nodes division and interaction process are shown in Fig. 5.

As shown in Fig. 5, when a client initiates a transaction to the Fabric network, first, the client needs to obtain legal identity from a certification authority to join the dedicated channel within the network, illegal devices are not allowed to access the network. At the same time, the collected original data information is processed by endorser peers in the gateway nodes. The endorser peers adopt the SHA-256 hash algorithm to generate a message digest, and encrypt the digest with the corresponding private key, the encrypted digital signature of the information sent to the orders peer. The orders are responsible for global sorting of all legitimate transactions in the network, and a batch of ordered transaction combinations are generated to a block structure, which is then sent to committer nodes for verification.

After the committer nodes receive the trading block regularly, they utilise the PBFT consistency protocol to check the message structure of the transaction, the integrity of the signature and whether it is repeated etc. When the verification pass, the legitimate request is executed and the result is written into the ledger, while the new block is constructed and link to the longest main blockchain. The data encryption and transmission process of IoT are shown in Fig. 6.

Each block is composed of a block header and a block body. The block header mainly stores the version number of the current block, the address of the previous block (Prev-block), timestamp, root value of Merkle tree etc. The block body mainly stores different types of data information. The structure of the data block is illustrated in Fig. 7.

Blocks are generated and connected into a chain one by one in chronological order. Each block is linked to each other through the hash address of the Prev-block header. The block body contains all collected and perceived information. Blockchain network composed of gateway nodes is formed by P2P networking technology, and the collected information is grouped and numbered by the distributed hash table and stored in the corresponding gateway nodes, so the data can be fast accurate position in the process of message transmission, to improve the efficiency of resource search and avoid malicious nodes send a large number of useless query requests that cause the CPU or bandwidth of the attacked gateway node is exhausted. As we know from Table 1, the verification and consensus mechanism of blockchain can effectively avoid the access of such malicious nodes.

In the meanwhile, the newly generated blocks are authenticated by PBFT consensus protocol before being linked to the longest main block chain. PBFT is a state machine replication algorithm. First, the state machine replicates copies of data information at different gateway nodes. The set of all copies of data information is represented by letter U, and each copy is represented by integer 0 to $|U| - 1$. It is assumed that the number of faulty network joints is f, and the number of network joints of the whole service is $3f + 1$. Then randomly choose a master node from all the gateway nodes to sort the data authentication requests. Other slave nodes execute authentication requests in the order provided by master node. The specific process of data authentication is as follows [22]:

(1) The master node broadcasts the selected data message to other slave nodes through serial number assignment messages, and other slave nodes send interactive messages if they accept, otherwise they do not send.
(2) Once $2f$ nodes receive the messages that interact with each other, then each node sends the serial number to confirm message.
(3) When $2f + 1$ nodes receive the ordinal confirmation message, it means that the data information is confirmed.

When other slave nodes find that the master node is a malicious node, the algorithm selects other slave nodes as master node. As shown in Fig. 8, four nodes are represented, C is the client, N_0 is the master node, N_1, N_2 is the slave node, and N_3 is the malicious node, which does not respond and send any messages. When the final node state reaches the serial number confirmation, it means that consensus has been reached in this round.

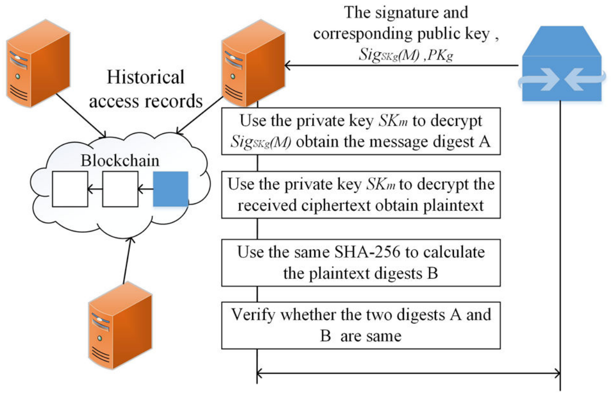
The signature and corresponding public key , $Sig_{SKg}(M)$,PKg
Historical access records
Blockchain
Use the private key SK_m to decrypt $Sig_{SKg}(M)$ obtain the message digest A
Use the private key SK_m to decrypt the received ciphertext obtain plaintext
Use the same SHA-256 to calculate the plaintext digests B
Verify whether the two digests A and B are same

Fig. 9 *Data decryption and validation process of IoT*

5.2 Data decryption and application of IoT

After receiving the signed information, the middleware servers need to verify the message to ensure its integrity in transmission. The corresponding middleware servers directly access the gateway nodes that send the message, use the private key it holds to decrypt the information, and then use the same SHA-256 hash function to calculate the information digests. Then decrypt the received digital signature with the public key held by the gateway node. If the two digests are same, middleware servers on the receiving side can confirm that the digital signature is held by the honest gateway node and has not been tampered with. If the transmitted data are slightly tampered, the string obtained through hash operation will change greatly, to ensure that the data block can be quickly identified when tampered, and finally ensure the integrity of the block. The decryption and verification process of data in IoT is shown in Fig. 9.

To verify the security of the data signature and decryption process in the blockchain-based IoT system. We adopt the Biba model [25], an integrity security model to carry out formal security verification. In this paper, because various encryption means in the data transmission can guarantee its security, we only emphasise data integrity and do not discuss the security level of information confidentiality. The verification process is shown as follows.

According to the strict integrity strategy of Biba model, the system in the integrity state that needs to meet the following requirements: allow middleware servers to view gateways with higher or equal integrity level; Modify the permissions of gateways with equal or below integrity level; Invoke other servers with equal or below integrity level. That is: if $I(s) \le I(g)$, then $\{r\} \in SG$, if $I(s) \ge I(g)$, then $\{w\} \in SG$, where the integrity level of servers s_i and gateways g_j is expressed as $I(s_i)$ and $I(g_j)$, the range of middleware access gateway is SG, where $\{r\}, \{w\}$ represent read and write operations to gateways, respectively.

We first give a theorem description of the information security characteristics after digital signature encryption.

Theorem: Let $I_{s\_\max} = \max_{s \in S}\{I(s)\}$ and $I_{g\_\min} = \min_{g \in G}\{I(g)\}$ respectively represent the maximum integrity level of all middleware servers and the minimum integrity level of all gateways. The following two conclusions hold true when middleware with access and decryption rights: No servers, including the middleware servers that implement the decryption, have right to change the signed information; As long as the middleware servers have right to access the information of gateway nodes, the servers can verify the validity of the signature.

Proof: $\forall g \in G$, $s \in S$ suppose that a server $s' \in S$ has the right to read the message m in the gateway g, the read and the decrypted message is $m' \in s'$, the accessed gateway $g' \in G$. Now we discuss the relationship between $I(s')$ with $I(g)$ and $I(s)$ with $I(g')$.

If middleware server s' has the right to read the information in the gateway g, server s' also has the right to decrypt the message in gateway g, then $I(s') \ge I(g)$. When decrypt the message and verify the validity of signature, it needs to verify the equation:

$$I(g') = I(g) + I_{s\_\max} - I_{g\_\min} + 1 \tag{1}$$

When $I(s') \ge I(g)$, $s \in S$ by the formula (1)

$$\begin{aligned} I(s) - I(g') &= I(s) - \left(I(g) + I_{s\_\max} - I_{g\_\min} + 1\right) \\ &= I(s) - I_{s\_\max} + I_{g\_\min} - I(g) - 1 \end{aligned} \tag{2}$$

Because $I(s) - I_{s\_\max} \le 0$, $I_{g\_\min} - I_g \le 0$, for any s, g, g' is true, the result <0 always holds, that is $I(s) < I(g')$.

This indicates that when middleware server s' has right to decrypt information in gateway node g, no servers (including s' itself) can change the signed information in gateway g', so the integrity of information is guaranteed; It is known $I(s) < I(g')$, any middleware server s has right to read information in gateway g, at the same time, when server s has right to read information of gateway g, middleware s can verify the signature of g by reading the information in g and g'.

When $I(s') < I(g)$, middleware server s' has no right to access the information in gateway, indicating that server s' has no right to decrypt the information in gateway g.

From the above, the theorem is proved. □

Since the information stored in gateway nodes is encrypted, and the middleware servers use the irreversibility and anti-collision of SHA-256 hash function to avoid denial, forgery, tampering and impersonation during its access and decryption verification, and timestamp can also ensure the integrity of historical data. Therefore, our proposed scheme can guarantee the confidentiality, integrity and non-repudiation of data.

6 Safety analysis and comparison

In this section, we briefly introduced some threat models and discussed the robustness of our scheme to their attacks. In the encryption phase, the elliptic curve digital signature algorithm (ECDSA) and SHA-256 hash algorithm can avoid such attacks. The randomness and anonymity of master node selection in the PBFT consensus protocol can reduce such attacks. Finally, the security of our scheme is analysed by game theory.

6.1 Encryption phase security

The ECDSA algorithm adopted in this paper is the application of the Elliptic curve cryptography (ECC) system in a digital signature. Compared with other signature algorithms (such as RSA and DSA), it has absolute advantages in anti-aggression and the highest security of unit bit, such as 160 – bit ECC has the same security strength with 1024 – bit RSA, DSA, and it has the advantages of small computation and fast processing speed [26]. Therefore, for data encrypted by ECDSA, due to the lack of the private key, the attacker cannot decrypt the message to obtain the original data. If an attacker launches a dictionary attack to guess the secret key, in our scheme, the secret key is calculated by the authentication centre based on the identity of the devices, so the attacker cannot get the message without knowing the private key. In addition, the anti-collision of the one-way hash function SHA-256 used in this article provides additional robustness to the system.

6.2 Validation phase security

As described in Section 5.1, each client's validation request is blindly and randomly mapped to one master node for request ordering. In addition, for each newly created block, n nodes are randomly selected as verifiers, where the value of n is generated randomly but has a certain relationship with the number of fault nodes f, that is, $n \ge 2f + 1$. This selection method can avoid the following attacks.

DDoS attack: A DDoS attack is more likely to occur if a set of authentication nodes is known in advance. Such attacks can disrupt blockchain or be launched from within or outside the network. The replaceability and random selection of verify nodes can significantly mitigate this attack. This is because the verification node set is random and anonymous before it participates in a consensus vote. In addition, each step of the voting process will receive feedback from other slave nodes. Therefore, it is almost impossible to launch a DDoS attack, which requires attacking all the nodes in the network to destroy the system.

Bribery or corruption of master or slave nodes: An example of such an attack is a malicious verifier bribed other master or slave nodes to accept and vote for an invalid block. Performing such an attack requires knowing the identity of the target node. The PBFT protocol anonymises the interaction between the consensus party and the verifier party. In addition, even if the randomly selected master node is malicious, the system can detect it due to the fault tolerance of the PBFT algorithm, to overcome this kind of attack.

6.3 System security analysis based on game theory

In this paper, blockchain was designed as a distributed system with multiple gateway nodes, it can ensure that attacks will not focus on centralised services. For a DDoS attack, the attacker must access multiple nodes at the same time, which makes the attack more difficult, time-consuming and expensive. To better evaluate the system architecture, we use game theory to analyse the security against some real attacks. We model the interaction between gateway devices and sensing devices as an incomplete information game to study the offensive and defensive game process under external attack.

In this paper, we use $G[N, \{T_i\}, p, \{S_i(t_i)\}, \{u_i\}]$ to represent incomplete information attack and defense game, where N is the set of players of the game, for this paper, $N = \{\text{gateway nodes, perception nodes}\}$. T_i is a set of type of participant i, there is only one type for gateway node, and for sensor nodes $T_i = \{\text{legal nodes, malicious nodes}\}$, p is the probability distribution of participants in all type spaces. $S_i(t_i)$ represents the set of policies available when participant i is of type t_i, when i is a gateway node, $S_i(\text{gateway node}) = \{\text{authentication, not authentication}\}$; When i is a legal node, $S_i(\text{legal node}) = \{\text{do not attack}\}$; When i is a malicious node, $S_i(\text{malicious node}) = \{\text{attack, do not attack}\}$. u_i represents the gain of player i in the game. The value of u_i is related not only to the strategies adopted by both sides of the game, but also on the type of game they belong to. Table 2 shows the definitions of some symbols used in this paper.

Table 2 System meaning

Symbol	Implication
w_1	The benefits that gateway node identify malicious node successfully; the loss that malicious node is identified.
w_2	The benefits that malicious node launch attack successfully; the loss that gateway node is attacked successfully.
α	The benefits of the gateway node receiving true information.
e_1	The energy cost of identifying malicious nodes that launch external attacks
e_2	The energy cost of sending messages by malicious nodes.
e_3	The energy cost of identifying malicious node that launched the internal attack.
x, x_1, x_2	Probability of a malicious node launching attacks.
y	Probability of gateway node authentication.
p_1	Probability that gateway node receives information from a legitimate node.
p_2, p_3	Probability that gateway node receives information from a malicious node.
Eu_1	Expected income of gateway node in offensive and defensive game.
Eu_2, Eu_3	Expected income of malicious node in offensive and defensive game.

Table 3 Game income table of gateway node and malicious node under external attack

Gateway nodes	Malicious nodes		Legitimate member nodes
	Attack	No attack	No attack
authentication	$w_1 - e_1, -e_2 - w_1$	$w_1 - e_1, -e_2 - w_2$	$\alpha - e_{1,} - e_2$
non-authentication	$-w_2, w_2 - e_2$	$\alpha, -e_2$	$\alpha, -e_2$

6.3.1 Game model and theoretical analysis:

In an untrusted network environment, malicious nodes may consume the verification resources of network nodes in the blockchain by frequently sending false data, so as to destroy the availability of the network. Although gateway nodes cannot confirm whether information is sent by a member node or a malicious node before receiving the verification information, it can judge the probability of the information sent by a certain node based on historical experience (assuming the probability of the information sent by an honest node is p_1 and the probability of the information sent by a malicious node is p_2).

After receiving the information, the gateway node can adopt two strategies of active authentication or passive non-authentication, while the malicious node can also adopt two strategies of attacking or not attacking. It should be pointed out that the non-attack strategy of a malicious node does not mean that it does not send any information, but that it sends the real information it perceives to the gateway node. The game payoff matrix of gateway node, malicious node and its member node is shown in Table 3.

Each time the gateway node performs authentication, it needs to consume a certain amount of energy and the cost is e_1. If it successfully detects the malicious nodes, it will generate income w_1 and cause the loss of w_1 for malicious nodes. If the gateway node does not carry out authentication and is attacked by malicious node, it will generate the loss w_2 and malicious node will gain w_2. When a malicious node does not attack and gateway node is negative authentication, the gateway node will receive the real useful information sent by the malicious node and generate income α; As for malicious node, it will send information regardless of whether it attacks or not, so it will generate energy consumption e_2; It should be pointed out that for external attacks, no matter whether the malicious node launches the attack or not, as long as gateway node authenticates it, it can be detected. In addition, to make the authentication and the attack behaviour meaningful, $w_1 > e_1$ and $w_2 > e_2$ should be satisfied.

As Table 3 shows, the attack strategy is the dominant strategy of the malicious node. Therefore, no matter whether gateway node conducts authentication or not, malicious node should adopt an attack strategy, and gateway node will certainly adopt authentication strategy at this time. Therefore (authentication, attack) is a pure Nash equilibrium strategy for gateway node and malicious node. In the game between gateway node and ordinary honest node, the member nodes only have one policy (no attack), and gateway node adopts non-authentication strategy as optimal strategy at this time. However, gateway node does not know which type of the sensing node is, we assumed that it adopts a mixed strategy, with probability y for positive verification and probability $1 - y$ for negative verification. Since the probability of gateway node knowing that the information sender is a legitimate member is p_1 and the probability of a malicious node is p_2, so (3) can be used to calculate expected revenue Eu_1 of gateway node

$$\begin{aligned} Eu_1 = {} & p_1 y(\alpha - e_1) + p_1(1 - y)\alpha + p_2 y(w_2 - e_1) \\ & + p_2(1 - y)(-w_2) \end{aligned} \tag{3}$$

Let $\partial Eu_1 / \partial y = 0$, that is

$$\begin{aligned} p_1(\alpha - e_1) - p_1\alpha + p_2(w_1 - e_1) \\ + p_2 w_2 = 0 \end{aligned} \tag{4}$$

because of $p_1 + p_2 = 1$, then we obtain

$$p_2 = \frac{e_1}{w_1 + w_2} \tag{5}$$

When $p_2 = e_1/(w_1 + w_2)$, $\partial Eu_1/\partial y = 0$, the expected revenue of positive authentication is equal to negative authentication. When $p_2 > e_1/(w_1 + w_2)$, $(\partial Eu_1/\partial y) > 0$, the expected revenue from active authentication of gateway node is higher than that from negative authentication. When, $p_2 < e_1/(w_1 + w_2)$, $(\partial Eu_1/\partial y) < 0$, the expected revenue from active authentication of gateway nodes is lower than that from negative authentication.

Therefore, the gateway node determines which strategy to pursue based on the value of p_2, which is related to attack frequency by the malicious node. As for malicious node, although it will adopt a pure strategy to attack, it must control its attack frequency to maximise its benefits, because when its attack frequency increases, the value of p_2 will also increase. When $p_2 > (e_1/w_1 + w_2)$, gateway node will actively adopt authentication strategy so that the income of malicious node is damaged. Supposing that attack frequency of a malicious node is φ, and when $\varphi = \varphi^*$, $p_2 = (e_1/w_1 + w_2)$, then malicious node will control its attack frequency and serve as $\varphi < \varphi^*$, the possibility of blockchain network detecting attacks is increased at this time. Although the system is in a passive authentication state, once a round of consensus is reached, malicious nodes can be identified and the system will refuse to respond to their subsequent requests. Therefore, it can be seen from the above analysis, no matter what strategy gateway node adopts, the scheme proposed in this paper can guarantee the security of the system. Even if more than one-third gateway nodes conspired to stop verification, system can also obtain the maximised utility, so as to reach an equilibrium state and avoid possible losses caused by misconduct or non-compliance with the protocol.

In Table 4, we briefly compare our approach with related blockchain-based IoT security works from the main security goals and functionality features. As for the table notation, *Y* and *N* indicate to 'provide' and 'not to provide' the property of security and functionality. Note that '∼' indicate the authors did not consider the relevant aspects. In addition, in [13], the approach relies on a public blockchain which transaction verification need a certain time. However, there are many real-time IoT application scenarios where this period is not tolerated. In [14], the authors focus on the data privacy protection of IoT devices, but does not consider data security. In [16], the local blockchains are not distributed but centralised which is contrary to its principle because it can limit its power and availability, and this research only aims to optimise blockchain in smart home, and does not discuss its application in other IoT domains. In [19], the authors utilise the powerful cloud servers for mining in the blockchain network, but this makes it vulnerable to a single point of failure. As you can see from above that our approach is much more secure, which makes our scheme more appropriate for IoT security.

7 Performance analysis

In this section, since the majority of the described works are in an experimental phase, where only the description of the approach is quickly provided and no implementations or simulations were realised, so it is very hard to compare our approach with related works on performance. Thus, we analysed the performance of our proposed scheme from the key parts that we rely on, which consist of computational complexity and communication capability. We also analysed the transaction throughput and communication latency of our proposed solution.

7.1 Computational complexity

The PBFT algorithm reduced the operational complexity of original Byzantine protocol from exponential to polynomial, thus from $o\left(n^{(f+1)}\right)$ inverted to $o\left(n^2\right)$ [22], and make it possible to apply in resource-constrained distributed IoT system.

7.2 Communication capability

Compared with [13–19], our proposed scheme makes full use of the processing speed and storage space of gateway devices, our scheme can quickly respond to requests, because the gateway can preprocess and filter data, thereby reducing transaction information latency and blocking problems that caused by unnecessary data authentication. In addition, since all data processing operations, such as encryption and storage, are carried out by gateway devices, the energy consumption of underlying sensor nodes is also reduced and battery life is improved. Therefore, our proposed scheme has a relatively robust communication capability.

7.3 Applicability of Hyperledger-Fabric for IoT

Hyperledger-Fabric adopts the modular architecture to build gateway nodes into a generic permissioned blockchain network to provide plug-and-play services for different IoT applications. Hyperledger-Fabric has less energy and computational requirements, high transaction throughput performance and low latency of transaction confirmation, it is more suitable for resource-constrained IoT devices.

We set up the blockchain network with peer nodes $n = 4$, order node $o = 1$, CA = 1 and fault node $f = 1$ using the IBM's Bluemix service, running an IoT application [27] developed by IBM Watson team. The transaction throughput and communication latency of our proposed solution are shown in Fig. 9.

As shown in Fig. 10, with the increasing of requests per second, although the time to consensus increases correspondingly, the increase is modest. While the transaction throughput has a relatively high increase. When requests per second reach about 250, the system's transaction throughput declines due to the increasing queuing delays for requests in the prepare and commit phases of PBFT. However, with the long-term operation of the IoT system, the number of nodes participating in the network increases gradually, and the Byzantine nodes tolerated by system increases dynamically, we can adopt sharding to process the transaction in parallel to solve the problem.

8 Conclusion and future work

In this paper, we addressed the problem of data security and privacy for billions of constrained devices in IoT. Certainly, the traditional networks can be protected by firewalls, static networks of IDS/IPS, and other peripheral defence mechanisms. However,

Table 4 Security/functionality features comparison

Attributes	[13]	[14]	[15]	[16]	[17]	[18]	[19]	Our scheme
decentralisation	*Y*	*Y*	*Y*	*N*	*Y*	*Y*	*Y*	*Y*
authentication	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
integrity	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
privacy	∼	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*	*Y*
non-repudiation	*Y*	*Y*	∼	∼	∼	*Y*	∼	*Y*
compatibility	*Y*	∼	∼	∼	∼	∼	∼	*Y*
confidentiality	∼	*Y*	*Y*	*Y*	*Y*	∼	*Y*	*Y*
security against DoS	*Y*	∼	∼	*Y*	∼	∼	*Y*	*Y*
immunity against node negative authentication	∼	∼	∼	∼	∼	∼	∼	*Y*

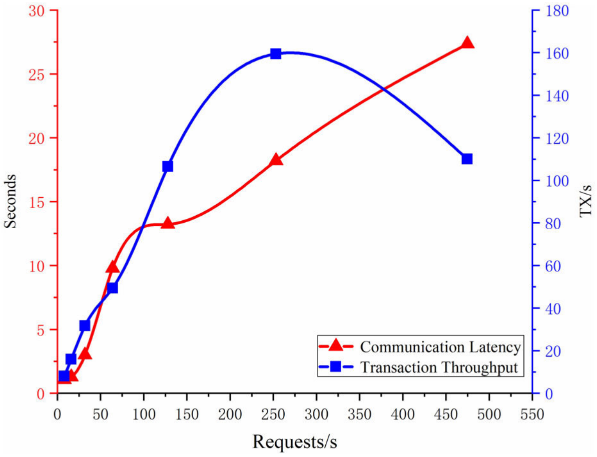

Fig. 10 *Transaction throughput and communication latency*

for the IoT devices with limited resources, the traditional network defence mechanism is difficult to protect the IoT devices against internal attacks and unauthorised damage. This paper introduces a new security defence mechanism to solve the security problem of numerous sensor data in IoT. The solution is fully decentralised and based on blockchain technology. Since the majority of IoT devices are largely constrained to store, analysis and process data, our scheme makes full use of gateway devices which makes it easier to encrypt and store numerous sensor data, and makes the blockchain technology adapt to the current IoT system.

The purpose of this paper is to provide a generic, secure, and easy-to-deploy security framework for IoT and to expound the operation mechanism of the IoT platform under Hyperledger-Fabric technology. Our solution can ensure the security and privacy of numerous sensor data. In general, our solution can adapt to most IoT scenarios, thus confirming that blockchain technology can be well embedded into IoT platform.

As future work, we will further study how to distribute gateway nodes in a large-scale heterogeneous IoT environment, to deploy blockchain network in a more secure and efficient way, thus simplifying the complexity of the system and reducing the deployment cost. And as can be seen from Fig. 10, when the number of requests exceeds a certain number, the system performance of our proposed scheme will be reduced due to the decrease of PBFT consensus efficiency, so we will optimise PBFT consensus protocol and formulate corresponding incentive mechanism to reduce the time to reach consensus, thus reduce unnecessary delays, and comprehensively consider the balance between energy consumption and safety requirements to achieve global optimisation. In addition, the integration of our proposed scheme with existing standards and development level of IoT is very important and should be studied in the future as well.

9 Acknowledgments

The authors thank the anonymous reviewers for their critical and constructive comments, their thoughtful suggestions have helped improve this paper substantially. This work was supported by the Scientific Research Project of Jilin Provincial Department of Education (project no. JJKH20170104KJ, JJKH20180418KJ).

10 References

[1] Rivera, J., van der Meulen, R.: 'Forecast alert: internet of things-endpoints and associated services'. Technical Rreport, December 2014

[2] Khan, M.A., Salah, K.: 'Iot security: review, blockchain solutions, and open challenges', *Future Gener. Comput. Syst.*, 2018, **82**, pp. 395–411

[3] 'Flashpoint. Mirai Botnet linked to Dyn DNS DDoS attacks'. Available at https://www.flashpointintel.com/blog/cybercrime/mirai-botnet-linked-dyn-dns-ddos-attacks, accessed 18 December 2018

[4] Ouaddah, A., Mousannif, H., Elkalam, A.A., *et al.*: 'Access control in the IoT: big challenges and new opportunities', *Comput. Netw.*, 2016, **112**, pp. 237–262

[5] Kouicem, D.E., Bouabdallah, A., Lakhlef, H., 'Internet of things security: a top-down survey', *Comput. Netw.*, 2018, **141**, pp. 199–221

[6] Mao, Y., Li, J., Chen, M.R., *et al.*: 'Fully secure fuzzy identity-based encryption for secure IoT communications', *Comput. Stand. Interfaces*, 2015, **44**, pp. 117–121

[7] Tan, S.Y., Yeow, K.W., Hwang, S.O.: 'Enhancement of a lightweight attribute-based encryption scheme for the internet of things', *IEEE Internet Things J.*, 2019, **6**, (4), pp. 6384–6395

[8] Aghili, S.F., Mala, H., Shojafar, M., *et al.*: 'LACO: lightweight three-factor authentication, access control and ownership transfer scheme for E-health systems in IoT', *Future Gener. Comput. Syst.*, 2019, **96**, pp. 410–424

[9] Prosanta, G., Biplab, S.: 'Lightweight and privacy-preserving two-factor authentication scheme for IoT devices', *IEEE Internet Things J.*, 2018, **6**, (1), pp. 580–589

[10] 'Nbakamoto, S-bitcoin: a peer-to-peer electronic cash system'. Available at www.bitcoin.org, accessed 2008

[11] Reyna, A., Martín, C., Chen, J., *et al.*: 'On blockchain and its integration with IoT. Challenges and opportunities', *Future Gener. Comput. Syst.*, 2018, **88**, pp. 173–190

[12] Minoli, D., Occhiogrosso, B.: 'Blockchain mechanisms for IoT security', *Internet of Things*, 2018, **1–2**, pp. 1–13

[13] Hammi, M.T., Hammi, B., Bellot, P., *et al.*: 'Bubbles of trust: a decentralized blockchain-based authentication system for IoT', *Comput. Secur.*, 2018, **78**, pp. 126–142

[14] He, Q., Xu, Y., Liu, Z., *et al.*: 'A privacy-preserving internet of things device management scheme based on blockchain', *Int. J. Distrib. Sens. Netw.*, 2018, **14**, (11), pp. 1–12

[15] Qian, Y., Jiang, Y., Chen, J., *et al.*: 'Towards decentralized IoT security enhancement: a blockchain approach', *Comput. Electr. Eng.*, 2018, **72**, pp. 266–273

[16] Dorri, A., Kanhere, S.S., Jurdak, R.: 'Towards an optimized BlockChain for IoT'. Proc. Int. Conf. Internet-of-Things Design & Implementation, Pittsburgh, PA, USA, April 2017, pp. 173–178

[17] Yu, Y., Li, Y., Tian, J., *et al.*: 'Blockchain-based solutions to security and privacy issues in the internet of things', *IEEE Wirel. Commun.*, 2018, **25**, (6), pp. 12–18

[18] Yu, B., Wright, J., Nepal, S., *et al.*: 'IoTChain: establishing trust in the internet of things ecosystem using blockchain', *IEEE Cloud Comput.*, 2018, **5**, (4), pp. 12–23

[19] Angin, P., Mert, M.B., Mete, O., *et al.*: 'A blockchain-based decentralized security architecture for IoT', in Georgakopoulos, D. (Ed.): '*Internet of things – ICIOT 2018*' (Springer, Cham, 2018), pp. 3–18

[20] Hassija, V., Chamola, V., Saxena, V., *et al.*: 'A survey on IoT security: application areas, security threats, and solution architectures', *IEEE Access*, 2019, **7**, pp. 82721–82743

[21] 'Hyperledger-fabric documentation'. Available at https://media.readthedocs.org/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf, last accessed 10 September 2018

[22] Castro, M., Liskov, B.: 'Practical byzantine fault tolerance'. Proc. Int. Conf. Operating Systems Design & Implementation, New Orleans, Louisiana, USA, 1999, pp. 173–186

[23] Makhdoom, I., Abolhasan, M., Abbas, H., *et al.*: 'Blockchain's adoption in IoT: the challenges, and a way forward', *J. Netw. Comput. Appl.*, 2018, **125**, pp. 251–279

[24] 'Hyperledger whitepaper'. Available at https://github.com/hyperledger/hyperledger/wiki/Whitepaper-WG, last accessed 13 September 2018

[25] Biba, K.: 'Integrity considerations for secure computing systems'. Mitre Report, 1975

[26] Johnson, D., Menezes, A., Vanstone, S.: 'The elliptic curve digital signature algorithm (ECDSA)', *Int. J. Inf. Secur.*, 2001, **1**, (1), pp. 36–63

[27] 'IBM Watson IoT Track and Trace contract'. Available at https://github.com/ibm-watson-iot/blockchain-samples/, last accessed 26 July 2019