scientific reports

Check for updates

OPEN

A decentralized authentication scheme for smart factory based on blockchain

Zhong Cao[1,3], Xudong Wen[1,3], Shan Ai[2], Wenli Shang[1]✉ & Sha Huan[1]✉

The Industrial Internet of Things (IIoT) is recognized as one of the revolutionary technologies driving smart manufacturing and improving productivity. As manufacturing processes grow increasingly intricate, the entire manufacturing ecosystem encompasses multiple managed IoT domains. Within this highly interconnected environment, devices from diverse domains must collaborate, leading to considerable apprehensions about the security and privacy of device-to-device communications. Current authentication methods encounter several challenges. Traditional authentication schemes overly rely on trusted third parties, rendering them susceptible to external attacks or internal spoofing. This susceptibility gives rise to a range of security and privacy concerns. In response to these challenges, this paper aims to contribute to a more secure and efficient service scheme for smart factories by devising a blockchain-based distributed IoT architecture. The proposed scheme introduces a federated blockchain to establish trust among different domains, thereby enabling secure connections between devices in distinct domains. Through security analysis, it is proved that the proposed authentication scheme has integrity, mutual authentication, scalability, and resistance to four attacks. Furthermore, efficiency analysis experiments show that our scheme is feasible for smart factories, and as the number of peer nodes increases, the performance and efficiency of the blockchain network become better.

Keywords Industrial Internet of Things, Smart factory, Decentralized authentication scheme, Internal spoofing, Federated blockchain

In recent years, with the introduction of the concept of Industry 4.0, the Industrial Internet of Things (IIoT) has been recognized as one of the means of realizing the concept[1]. The realization of Industry 4.0 is dependent on Internet of Things (IoT) technology, while IIoT provides the device connectivity and data foundation needed for Industry 4.0, and together they are driving the digital and intelligent transformation of modern manufacturing[2,3].

One of the goals of Industry 4.0 and IIoT is to create smart factories, which use advanced digital technologies such as the IoT, Artificial Intelligence (AI), and Blockchain to connect sensors, devices, and systems to digitize and smarten the production environment[4]. Key benefits include real-time monitoring, automated production, predictive maintenance, quality control, and resource optimization. This enables factories to improve efficiency, quality, and competitiveness while reducing costs and environmental impact. In this context, production processes often span multiple systems, which may be located in different geographical areas with independent functions and data. In order to manufacture a complete product, these systems need to cooperate, and devices located in different systems need to communicate with each other to enable real-time data sharing and collaborative decision-making for more effective information exchange and collaboration[5]. The architectural design and technical support of smart factories enable manufacturing companies to achieve cross-system and cross-geographical co-production and seamless integration of production processes. This brings higher productivity, faster time-to-market, and more flexible production responsiveness to the manufacturing industry.

In smart factories, device authentication information management and IoT multimedia data privacy are becoming more and more important. Yang et al.[6] proposed a privacy protection method based on deep learning and Mahalanobis distance, which provides an effective solution for privacy protection in smart factories. While devices in different systems can be easily connected through widely used network infrastructures, ensuring secure communication between them is a critical task. For example, plant administrators do not want any device from another system to access their equipment without authentication. Currently, most authentication mechanisms rely on traditional public key infrastructure (PKI) systems. However, PKI systems face complex

[1]School of Electronics and Communication Engineering, Guangzhou University, Guangzhou 510006, China. [2]School of Artificial Intelligence, Guangzhou University, Guangzhou 510006, China. [3]These authors contributed equally: Zhong Cao and Xudong Wen. ✉email: shangwl@gzhu.edu.cn; speeshuan@gzhu.edu.cn

certificate management, high operation and maintenance costs, and their centralized architecture has many vulnerabilities that lead to security and trustworthiness issues, especially in multi-party environments[7]. In addition, PKI's authentication limitations and trust in certificate authorities pose challenges.

In smart factory environments, traditional authentication mechanisms have become overstretched as the diversity of devices and the need for interconnectivity increase. Therefore, there is an urgent need for a more secure and decentralized authentication mechanism to address these challenges. Blockchain, as a decentralized technology with features such as tamper-proof, traceable, and open and transparent, can provide a new solution to the security problem of IoT[8,9]. These features are particularly suitable for smart factories, which can ensure secure communication and data sharing between devices, thereby improving productivity and safety.

Blockchain technology has been widely used in multiple solutions, but its application in IoT security is still in the exploratory stage, and existing blockchain-based approaches face many challenges. Smart factories have an urgent need for fast and efficient device authentication, which makes choosing the right type of blockchain especially important. Blockchains can be categorized into public, private and federated blockchains. Public blockchains are completely open and decentralized for scenarios that require transparency and do not rely on trusted centers, but have performance limitations and privacy protection issues. Ether is a typical public blockchain, and although many studies[10–13] have utilized it to build networks, it is unsuitable for the fast and efficient device authentication needs of smart factories due to slow transaction processing and high costs. Private blockchains are controlled by a specific entity, provide better performance and privacy protection, and are suitable for internal data management, but lack decentralization features and are not suitable for decentralized authentication. A federated blockchain[14] combines the advantages of both and is suitable for cross-organizational collaborative projects, enabling decentralization and data sharing while protecting privacy. It is maintained by multiple cooperative nodes, which need to be verified, and the participants work together through contractual constraints without complete trust in each other, thus ensuring the security and trustworthiness of device identities in smart factories.

In this paper, we propose a blockchain-based secure authentication scheme for cross-system IIoT devices. The scheme uses a consortium blockchain to establish trust between different systems, where each system has one or more representative nodes responsible for maintaining a global ledger. The main objective is to store the authentication results in the federation chain while enabling the authentication of IIoT devices.

The main contributions of this paper are as follows:

- Our proposed scheme supports the authentication of devices located in different IIoT systems, adopts a decentralized architecture, eliminates the need for a single authority, and effectively avoids traditional unilateral failures.
- Each system provides multiple nodes that form a blockchain network. All nodes of the decentralized network can participate in the management and the relationship between nodes is equal. If a node fails, it does not affect the normal operation of the network.
- We use smart contracts in our solution and the entire request process is executed by interacting with the smart contract. We used Hyperledger Fabric platform to implement our solution to evaluate the feasibility.
- The proposed scheme is analysed for security and efficiency, which improves security by sacrificing some performance and can be applied to authentication scenarios with high security requirements.The remainder of the paper is organized as follows. In "Related work", we recall the certificate-based authentication, key negotiation authentication, and blockchain-based authentication. In "System model", we introduce the scheme of the adopted federation chain platform. Then we present our bockchain-based authentication scheme in "Proposed scheme". Security analysis of the proposed scheme is given in "Evaluation". A relevant discussion based on the performance of the proposed scheme is given in "Discussion". Finally, the full text is summarized in "Conclusion".

Related work

Many authentication schemes for IoT applications already exist, including digital certificate-based authentication, key negotiation authentication, and blockchain-based authentication.

Certificate-based authentication

Choi et al.[15] proposed a certificate-based authentication system for IIoT applications using auxiliary network devices. The user's signature key is encrypted and this encryption process is computed using the user's password and a secret parameter in the auxiliary device to securely protect the signature key. The authors in[16] proposed a two-stage certificate-based implicit authentication scheme for WSNs in IoT applications, where cryptographic credentials are stored in the edge nodes. However, this design makes the mechanism vulnerable to cloning attacks. In[17], the authors designed a new certificate-based device access control scheme for IoT environments that is not only resilient to a wide range of attacks but also retains anonymity property. Many other certificate-based schemes[18,19] exist that provide much support in maintaining PKI and implicitly trust certificate authorities (CA). However, CAs are vulnerable to potential attacks and prone to operational errors, and CA failures have been observed globally[20].

Key negotiation authentication

To better suit the authentication of decentralized devices, symmetric keys are often negotiated using key exchange protocols to secure communications. This type of protocol reduces overhead by incorporating authentication into the key negotiation process, eliminating the need for digital certificates. The authors in[21,22] proposed a authentication protocol for constrained devices in machine-to-machine communication in IIoT. Lu et al.[23] proposed an edge-assisted authentication scheme that leverages the Information Center Network (ICN)

model to secure IIoT devices and reduce the burden on resource-constrained devices. Nosouhi et al.[24] proposed a security mechanism for wireless spoofing attacks in the Next Generation Internet of Things (NGIoT) that utilizes the beam characteristics of millimeter-wave devices for anomaly detection and ensures the identification of legitimate devices. Some related research[25–27] applied bioinformatics or bilinear pairing techniques to key agreements to facilitate authentication between user devices and IIoT devices or servers. In addition, many studies[28–30] proposed the use of servers to facilitate mutual authentication between two resource-constrained IIoT devices. However, key-negotiated authentication schemes often rely on a central entity (e.g., a gateway or key server). If this central entity fails or is attacked, the key management of the entire system may be compromised, thus threatening the security of all parties involved. Moreover, as the system scales, a centralized key negotiation system may face performance bottlenecks and scalability issues.

Blockchain-based authentication

Recently, researchers explored the use of blockchain technology with decentralized features to provide new authentication and security solutions for distributed IoT systems. Cui et al.[31] proposed a blockchain-based multi-WSN authentication scheme for IoT, which integrates different types of nodes by constructing a hybrid blockchain model, including local and public chains, to achieve mutual authentication of identities between nodes in various communication scenarios. Kumari et al.[32] proposed a novel public auditing mechanism that utilizes blockchain technology to ensure the integrity and transparency of healthcare data, providing strong support for authentication. The scheme demonstrates the potential of blockchain in ensuring data security and improving auditing efficiency. Reference[33] discusses how to enhance the security of data storage through post-quantum security mechanisms while utilizing blockchain for identity authentication and data auditing, demonstrating that blockchain technology can effectively address the security challenges in authentication, especially in highly sensitive data environments. Prajapat et al.[34] proposed the application of blockchain in secure authentication of IoT devices, emphasizing the importance of quantum security technology in protecting identity information. Gong et al.[35] proposed a blockchain based authentication framework for IIoT devices. In their proposed system, blockchain is used to store device identity information and a Blockchain of Things (BCoT) gateway is introduced to record authentication transactions. Reference[36] introduced an authentication scheme that leverages gateway nodes and Blockchain technology for IIoT devices. This approach incorporates gateway nodes to address the computational limitations and resource constraints of IIoT devices. The above study provides important insights into our proposed blockchain-based authentication scheme and shows that it is necessary to introduce advanced security techniques in industrial IIoT device authentication.

System model

We propose a Hyperledger Fabric-based federated blockchain model for building a trusted distributed network of smart factories integrating multiple industrial system nodes. The model leverages the identity management and X.509 certificate-based authentication mechanism of the fabric to manage participant identities through Member Service Providers (MSPs) and accurately manage permissions through policy-based access control. Channel segregation ensures that private transactions are shared only among authorized participants for enhanced security. Smart contracts support cross-system IIoT device authentication and securely store the results on the blockchain, ensuring transparent, consistent and trusted data. The designed blockchain-based distributed IIoT architecture is shown in Fig. 1, which mainly consists of four core components: sequencing service, channel, execution unit and IIoT device.

The ordering service consists of independent ordering nodes, which are responsible for receiving, ordering, and packaging transactions, and distributing transaction blocks to all nodes in the network to ensure the consistency of the transaction order so as to maintain the reliability and accuracy of the system.

The execution unit consists of a CA server, which consists of an organizational CA that generates digital certificates for different entities in the system, and a TLS CA that protects communication between nodes, and a peer node. Peer nodes, on the other hand, are responsible for storing the ledger, executing smart contracts, and maintaining the network state, and can play different roles as endorsing nodes and submitting nodes.

IIoT devices are connected to actuation units covering sensors, controllers and actuators for real-time data transfer and analysis, ensuring data security and integrity.

Channels provide logically isolated communication environments that allow participants to conduct transactions and authentication within separate channels, guaranteeing that transactions are visible only to specific systems. At the same time, the channel supports information sharing and facilitates the exchange of information necessary for the device during the authentication process. Peer and sequencing nodes involved in authentication are required to join one or more channels to maintain the order and consistency of authentication transactions for IIoT devices.

Proposed scheme

Blockchain-based authentication scheme

This section describes in detail the proposed scheme for cross-system device authentication, which is divided into three phases, and the detailed procedures for each phase are described below.

System initialization and device registration phase

When the devices in the system join the network, it is necessary to use the CA to issue a unique identity certificate for each device, including the TLS certificate, CA root certificate, private key, public key, identity information, certificate validity period, etc., and digitally signed by the CA to ensure the authenticity of the certificate.

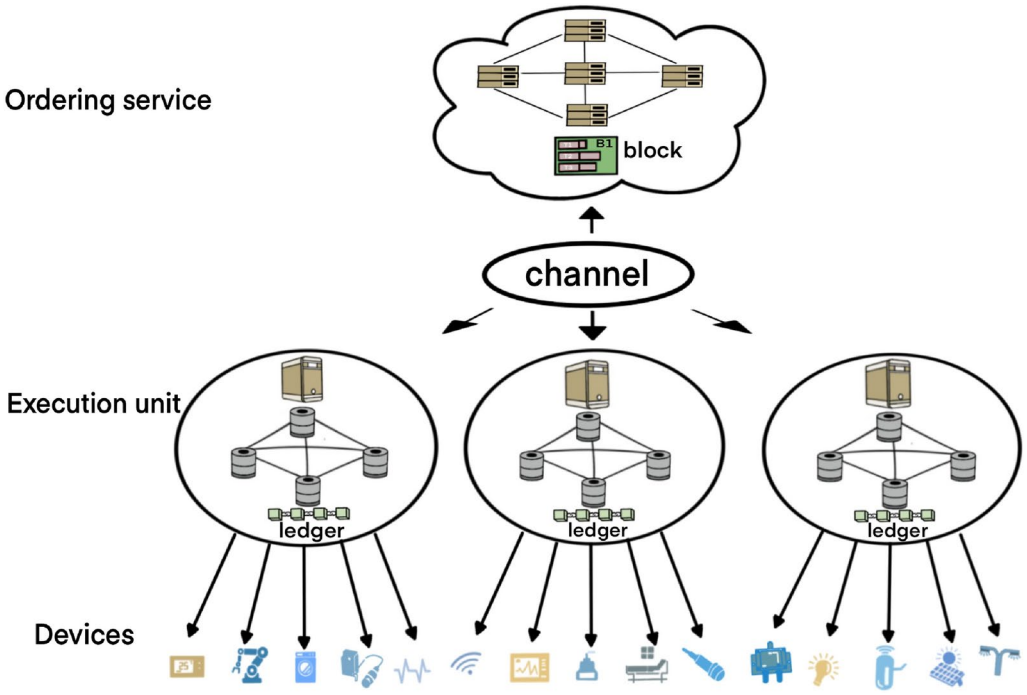

Fig. 1. Smart factory architecture.

Once the IIOT device has collected the aforementioned certificates, it can initiate a transaction request to the network, thereby registering the device on the blockchain. Upon successful registration, the identity of the device will be recorded in the blockchain ledger. The steps are as follows.

1. The peer node first checks whether the device initiating the registration request has permission to invoke the smart contract, usually using certificates for authentication.
2. Secondly, the device's certificate is checked for expiry. If the certificate has expired, the registration process will stop and an error notification will be returned.
3. The transaction is then validated by checking if the given device ID exists in the blockchain ledger, if it already exists in the ledger, the transaction will not be allowed and the registration process will stop with an error notification.
4. If the device ID does not exist in the blockchain ledger, the smart contract will allow the registration transaction and write the device information to the blockchain ledger, which contains a mapping of $\{ID, Owner, ExpirationTime\}$.Algorithm 1 describes this rule for the device registration phase.

Data: The information of the device that initiated the request
Result: Write device identity information to the blockchain ledger
// Parse from certificates
while *The device has permission to access the Smart Contract* **do**
  if $Timestamp > ExpirationTime$ **then**
    return *error()* ;
  end
  if $DeviceExists(ID, blockchain) = true$ **then** // Checking if the device ID exists in the blockchain ledger
    return *error()*
  else // Upload mapping blocks to blockchain ledger
    $create\_mapping(ID_i, Owner, ExpirationTime)$;
  end
end

Algorithm 1. Device registration rules for smart contract

Device-to-device authentication phase
Whenever a registered device (e.g. D_i) wants to communicate with another device (e.g. D_j), they need to securely share data after mutual authentication. The steps are as follows.

1. peer nodes likewise need to first check whether the device initiating the authentication request has permission to invoke the smart contract. Next, it has to check whether the two devices are registered in the blockchain and if they are registered, it moves to the next step.
2. After obtaining the identity information of both devices in the blockchain ledger, in order to prevent duplicate authentication, it is necessary to first check if the mapping block already exists. If it does not exist, the process continues by checking whether the devices are expired or not, and if one of the devices is expired, the authentication process stops due to an error. Otherwise, the process continues to the next step.
3. We establish a bi-directional connectivity relationship between two devices by adding two new mappings to the blockchain ledger.Algorithm 2 describes this rule for the device-to-device authentication phase.

Data: The information of the device D_i that initiated the request; ID_j of the device D_j wants to connect to
Result: Write added mappings to the blockchain ledger
// Parse from certificates
while *The device has permission to access the Smart Contract* **do**
  if $DeviceExists(ID_i, ID_j, blockchain) = true$ **then**
    // Reading device D_i identity information from blockchain ledger
    $D_i = ReadIDentity(ID_i)$
    if $D_i.Connection\_device = ID_j$ **then**
      return *error()*
    end
    $D_j = ReadIDentity(ID_j)$
    if $Timestamp < D_i.ExpirationTime$ ***and*** $Timestamp < D_j.ExpirationTime$ **then**
      // Adding new mappings to the blockchain ledger
      $D_i.Connection\_device = ID_j$
      $D_j.Connection\_device = ID_i$
    else
      return *error()*
    end
  end
end

Algorithm 2. Device-to-device authentication rules for smart contract

Device revocation phase
When a device expires or is damaged, we need to remove that device's information from the blockchain ledger, and at the same time, the connection associated with that device is disconnected. The steps are as follows.

1. Only the administrator of the system to which the device belongs has permission to delete the device, so you need to check whether the user calling the smart contract has administrator privileges first.
2. Reads the ledger data of the device to be deleted and information about the devices connected to that device.
3. Remove the information about the device from the block two ledger and disconnect the associated connection.Algorithm 3 describes this rule for the device revocation phase.

Data: ID_i of the device D_i want to delete
Result: Remove the information about the device D_i
// Parse from certificates
while *Users have system administrator privileges to access smart contracts* **do**
  // Read information about the devices connected to this device
  $D_j = ReadIDentity(Connection\_device = ID_i)$
  // Disconnect from the device D_i
  $D_j.Connection\_device = empty$
  $DeleteDevice(ID_i)$
end

Algorithm 3. Device revocation rules for smart contract

```
/peer0.org2.example.com/tls/ca.crt" -c '{"function":"Connectdevice","Args":["device2@org1"]}'
2023-10-30 19:46:56.118 CST 0001 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> Chaincode invoke su
ccessful. result: status:200
/peer0.org2.example.com/tls/ca.crt" -c '{"function":"Connectdevice","Args":["device3@org2"]}'
2023-10-30 19:48:24.165 CST 0001 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> Chaincode invoke su
ccessful. result: status:200
C mychannel -n basic -c '{"Args":["GetAllIdentity"]}'
[{"ID":"device1","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":"device3@org2"}
,{"ID":"device2","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":"device4@org2"}
,{"ID":"device3","owner":"org2","time":"2033-10-27T11:00:00Z","connection_device":"device1@org1"}
,{"ID":"device4","owner":"org2","time":"2033-10-27T11:00:00Z","connection_device":"device2@org1"}
]
```

Fig. 2. Device registration in blockchain.


```
/peer0.org2.example.com/tls/ca.crt" -c '{"function":"Connectdevice","Args":["device2@org1"]}'
2023-10-30 19:46:56.118 CST 0001 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> Chaincode invoke su
ccessful. result: status:200
/peer0.org2.example.com/tls/ca.crt" -c '{"function":"Connectdevice","Args":["device3@org2"]}'
2023-10-30 19:48:24.165 CST 0001 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> Chaincode invoke su
ccessful. result: status:200
C mychannel -n basic -c '{"Args":["GetAllIdentity"]}'
[{"ID":"device1","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":"device3@org2"}
,{"ID":"device2","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":"device4@org2"}
,{"ID":"device3","owner":"org2","time":"2033-10-27T11:00:00Z","connection_device":"device1@org1"}
,{"ID":"device4","owner":"org2","time":"2033-10-27T11:00:00Z","connection_device":"device2@org1"}
]
```


Fig. 3. Device authentication in blockchain.

```
example.com/tls/ca.crt" -c '{"function":"DeleteDevice","Args":["device4"]}'
Error: endorsement failure during invoke. response: status:500 message:"The submitting client is not
 an administrator and is not authorized to delete devices"
example.com/tls/ca.crt" -c '{"function":"DeleteDevice","Args":["device4"]}'
2023-10-30 19:59:20.448 CST 0001 INFO [chaincodeCmd] chaincodeInvokeOrQuery -> Chaincode invoke succ
essful. result: status:200
mychannel -n basic -c '{"Args":["GetAllIdentity"]}'
[{"ID":"device1","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":"device3@org2"},{
"ID":"device2","owner":"org1","time":"2033-10-27T11:00:00Z","connection_device":""},{"ID":"device3"
,"owner":"org2","time":"2033-10-27T11:00:00Z","connection_device":"device1@org1"}]
```

Fig. 4. Device revocation in blockchain.

Scheme implementation

This section details how to implement the proposed scheme using smart contracts developed in Golang. To ensure the correctness and validity of the smart contract, we validate it in a test network that comes with the Hyperledger Fabric 2.4 platform. This test network contains two organisations, each with a peer node, in addition to a separate ordering node responsible for consensus. By running smart contracts in this environment, we are able to fully evaluate their performance and effectiveness in real-world applications.

We registered four devices belonging to two different systems. Figure 2 shows the information written in the blockchain ledger after the successful registration of the device. After that, we completed mutual authentication between devices belonging to different systems. Figure 3 shows the output of the device after successful authentication. When we want to undo a device, we need to have administrator privileges, otherwise

the request is not allowed. Figure 4 shows the output when a device is revoked, from which it can be seen that the information about the device has been removed from the blockchain ledger and the connection associated with it has been disconnected.

Evaluation

Security analysis

In order to ensure the safe and effective operation of IoT and the security and trustworthiness of services, key security requirements must be met in the scheme design. In this section, a comprehensive security assessment of the proposed authentication scheme is conducted, especially for the common cyber attacks in IoT, and compared with existing works with similar objectives. The comparisons are provided in Table 1.

Integrity

Accuracy and tamper-proofness of data is the key to guaranteeing the safe operation of smart factories. The correctness of device authentication information is directly related to the trust and normal operation between devices. If this information is tampered with, it may not only lead to system failure, but also trigger security risks such as unauthorized device access, thus affecting productivity and data security. Therefore, it is particularly important to ensure data integrity.

In our proposed scheme, data integrity is guaranteed through multi-layered security measures. Firstly, data is stored and transmitted using AES symmetric encryption, which, combined with Hyperledger Fabric's permission control mechanism, ensures that only authorised users and devices can access and modify the data. Second, transactions are signed using ECDSA digital signature technology to ensure that data is not tampered with during transmission across the network. In addition, we hash transaction data using hash functions such as SHA-256 to provide additional integrity checks and ensure that any data changes are detected in a timely manner.

Mutual authentication

Mutual authentication is the foundation for ensuring that devices in a smart factory communicate securely. By establishing a relationship of trust, devices can ensure each other's identity, thereby preventing unauthorized access and potential security threats. Effective mutual authentication not only protects the security of data transmission, but also provides reliable collaboration between devices.

Each device holds a license digitally signed by a trusted authority and uses its license to authenticate itself to the blockchain network. From this, only valid devices can complete the authentication correctly. Finally, the information about the mutual authentication of the two devices is recorded in the blockchain ledger.

Scalability

In IIoT environments, scalability faces many challenges. As the number of devices proliferates, the complexity of managing and authenticating legitimate devices increases significantly. Traditional centralized authentication methods may not be able to efficiently handle large-scale device registration and authentication requests, leading to performance bottlenecks. In addition, the simultaneous connection of a large number of devices can lead to network congestion, increase latency, and affect the reliability of real-time data transmission. At the same time, security and trust issues are becoming more and more prominent, and the access of illegal devices may threaten system security.

To cope with these challenges, this paper proposes to use blockchain technology to record the authentication information of devices. The decentralized nature of blockchain ensures the non-tamperability of each device's identity and efficiently handles large-scale authentication requests through a consensus mechanism, thus improving the scalability of the system. To cope with the access problem of invalid devices, we establish an effective revocation mechanism to ensure that the system remains secure and reliable in the changing device environment.

Resistance to replay attack

Resistance to Replay Attack is an important measure to ensure the security of smart factory systems. Attackers may utilize submitted transactions to send duplicate requests to the network, which not only leads to a waste of resources, but also may cause serious security risks and affect the normal operation of the system. Therefore, it is crucial to take effective protection measures.

Security properties	Patel et al.[29]	Dang et al.[30]	Panda et al.[36]	Almadhoun et al.[37]	Proposed
Mutual authentication	✓	✓	✓	✓	✓
Scalability	✓	✓			✓
Resists MITM attack	✓	✓	✓	✓	✓
Resists DDOS attack			✓	✓	✓
Resists replay attack	✓	✓		✓	✓
Cross domain authentication			✓		✓
Decentralization			✓	✓	✓

Table 1. Comparison of security attributes.

In our scheme, each transaction contains a timestamp, which effectively prevents replay attempts using the same or expired timestamps. At the same time, the unique transaction ID of the transaction and the tamperability of the blockchain ensure the integrity and traceability of the transaction history, preventing tampering or repeated attempts on submitted transactions. The combination of these mechanisms can effectively resist replay attacks and safeguard the security and stability of the system.

Resistance to man-in-the-middle (MITM) attacks
Resistance to man-in-the-middle (MITM) attacks is key to securing smart factory communications, as attackers may eavesdrop or tamper with information during communication, leading to data leakage or manipulation of equipment. Therefore, ensuring the confidentiality and integrity of communications is critical.

In our scheme, by encrypting the communication between nodes using the TLS protocol, we can effectively prevent intermediaries from eavesdropping and tampering with transactions. Only the nodes with the corresponding private keys can decrypt and authenticate the communication, thus ensuring the secure transmission of information.

Resistance to impersonation attack
Resistance to impersonation attacks is an important part of securing a smart factory. Attackers may attempt to masquerade as legitimate devices to gain access to the system, which not only jeopardizes data security, but can also lead to equipment failure and production interruptions. Therefore, it is critical to ensure the authenticity of device identity.

In our scheme, IIoT devices are authenticated through the use of digital certificates and private keys. Each device has a unique digital certificate and private key issued and managed by a trusted CA. This mechanism ensures the uniqueness and authenticity of the device, effectively prevents attackers from imitating the identity of the device, and safeguards the security and reliability of the system.

Resistance to distributed denial of service (DDoS) attacks
Resistance to distributed denial of service (DDoS) attacks is an important strategy to ensure the normal operation of smart factories. Attackers consume system resources through a large number of requests, resulting in service interruption or failure to operate normally. If the target device is the central node of a centralized system, its failure will have a serious impact on the entire system. Therefore, it is especially necessary to establish an effective protection mechanism.

In our proposed approach, DDoS attacks can be effectively defended by mechanisms such as channel isolation, load balancing, and high availability. Channel isolation assigns different IoT devices to different channels, thus narrowing the impact of DDoS attacks to specific channels without affecting the entire network. At the same time, load balancing and high availability ensure that the network is able to evenly distribute traffic and quickly switch to backup nodes in the event of an attack, thus maintaining continuity of authentication services. This comprehensive architecture significantly improves the system's resistance to DDoS attacks.

Cross-domain authentication and decentralisation
Cross-domain authentication is an important means of ensuring secure cooperation between different organizations. As IoT devices and services continue to expand, trust relationships between multiple organizations become increasingly complex. Effective cross-domain authentication protects data and resources from the threat of unauthorized access by ensuring that only authenticated members have access to the network.

In our scheme, cross-domain authentication manages user identity through certificate authorities and digital certificates to establish cross-domain trust. Meanwhile, decentralization is reflected in the distributed network structure and consensus mechanism, which avoids a single point of failure and ensures that each node enjoys equal status in transaction verification and ledger maintenance. And the execution of smart contracts further enhances the application logic of decentralization. Together, these features ensure the security and stability of the network and enhance the reliability of the overall system.

Efficiency analysis

The number of ordering nodes and peer nodes both affect network performance, but they have different roles and points of influence. Ordering nodes are responsible for consensus, and increasing their number can improve the fault-tolerance of the network and prevent single point of failure, but they may also increase the communication delay, thus affecting the overall processing speed. Peer nodes are responsible for maintaining the ledger and executing the chain code, and increasing their number can improve parallel processing and enhance overall throughput. However, more peer nodes may also increase the data distribution time, thus affecting the transaction processing speed. Therefore, in some cases, performance optimisation may focus on peer nodes.

For this purpose we set up an experiment which deploys a blockchain network on multiple cloud servers, each running multiple peer nodes and orderer nodes, and observe its impact on the system performance by varying the number of peer nodes. The various parameters of the experimental environment are shown in Table 2. We use the Hyperledger Caliper performance testing framework, which can be used to stress test the Hyperledger Fabric and output detailed performance metrics reports. In addition, we use Prometheus to continuously collect system resource usage during Caliper testing to get a comprehensive view of how the network performs under high load. We evaluated three different transaction requests, i.e., device registration, device authentication, and device revocation, and averaged their results. The experimental results are shown in Table 3.

Transaction latency is the time from when a user submits a transaction request until the transaction is confirmed on the blockchain and written to the ledger. As can be seen from the Table 3, the average transaction latency of the three transaction requests is relatively low at the beginning, but increases significantly with the

Name	Data
CPU	2 vCPU
Memory	2 GiB
OS	Ubuntu 22.04
Blockchain	Hyperledger Fabric 2.4
Monitoring Tools	Hyperledger Caliper, Prometheus

Table 2. The parameters of the experimental environment.

Number of peer nodes	Transaction Latency (ms)	Throughput (TPS)	Ledger synchronization time (ms)	Resource consumption (CPU)
3	192	462.6	138	36% CPU
6	235	488.4	169	42% CPU
10	296	531.7	206	53% CPU
15	354	622.9	291	60% CPU
20	470	702.4	375	79% CPU
25	655	685.3	504	91% CPU
30	886	679.7	676	99% CPU

Table 3. The effect of number of Peer nodes on performance.

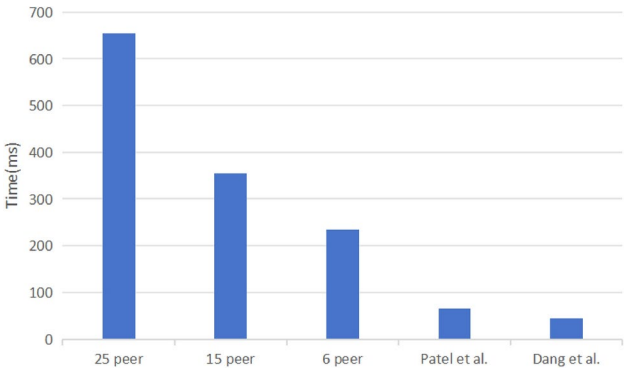

Fig. 5. Comparison time with centralized scheme.

number of nodes, especially after 20 nodes, when the latency increases to 470 ms. Ledger synchronization time is the time required to propagate and synchronize transaction data across multiple peer nodes, and it also increases with the number of Peer nodes, indicating that more nodes take longer to synchronize the ledger data. Throughput indicates the number of transactions that can be processed per second. As can be seen in Table 3, the average throughput of these three transaction requests peaks during the addition of nodes and levels off or even decreases slightly after 20 nodes, indicating that too many nodes may lead to a performance bottleneck. Resource consumption rises significantly with the number of Peer nodes, especially when the number of nodes reaches 30, CPU resources reach almost 100% utilization.

Discussion

It can be seen that increasing the number of peer nodes usually improves the throughput of the system to some extent, as more nodes are able to process and validate transactions in parallel. However, as the number of nodes increases, the transaction processing time also increases significantly. This is due to the fact that each node needs to be involved in the consensus process and the synchronization of the ledger, resulting in an overall longer processing time. Therefore, this throughput improvement is not linear, and as the number of nodes increases, the system performance is gradually limited by the network communication overhead and synchronization time. Therefore, when designing a blockchain system, a reasonable balance should be found between the number of nodes, throughput, transaction processing time, and resource consumption to ensure that the system maintains efficient operation while scaling.

In addition, we compare it with centralised authentication schemes[29,30] and the results are shown in Fig. 5. It can be seen that centralized authentication has a shorter response time, but this does not mean that it is more reliable as it can be easily attacked and compromised. The scheme proposed in this paper has higher time

complexity, but it is more secure, robust, and fault-tolerant, and is more suitable for application scenarios with high security requirements.

Conclusion

In this paper, we propose a novel blockchain-based distributed authentication scheme specifically for industrial IIoT devices. Our scheme utilizes multiple resourceful nodes to build a federated blockchain and adopts Hyperledger Fabric as a trusted platform.Authentication of IIoT devices is achieved through the development of smart contracts that ensure integrity, mutual authentication, scalability, and protection against four types of attacks. Through our analysis, we confirmed the effectiveness of the authentication solution, highlighting its security features, efficiency and scalability. This solution not only addresses the challenges associated with authenticating IIoT devices across different systems and locations, but also provides a reliable framework for smart factories to support their secure operations and data management. For example, Schneider Electric uses blockchain technology to manage device identity and security authentication in its smart manufacturing solution, automating the authentication process through smart contracts and significantly improving operational efficiency. In addition, Boeing uses blockchain in its aerospace manufacturing to track the origin and identity of parts. By recording device authentication information on the blockchain, Boeing is able to improve the security and transparency of its manufacturing process. These real-world examples further validate the effectiveness and feasibility of our proposed scheme in a smart factory environment.

In summary, our research provides an important reference and support for the safe and efficient operation of smart factories, demonstrating the prospect of a wide range of applications of blockchain-based authentication schemes in the industrial IIoT space. This scheme not only improves equipment security, but also paves the way for the digital transformation of smart factories, driving them towards a more efficient and trustworthy future.

Data availibility

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 15 August 2024; Accepted: 10 October 2024
Published online: 20 October 2024

References

1. Lasi, H., Fettke, P., Kemper, H.-G., Feld, T. & Hoffmann, M. Industry 4.0. *Bus. Inf. Syst. Eng.* **6**, 239–242 (2014).
2. Wu, Y., Dai, H.-N. & Wang, H. Convergence of blockchain and edge computing for secure and scalable IIoT critical infrastructures in industry 4.0. *IEEE Internet Things J.* **8**, 2300–2317 (2020).
3. Shen, M., Deng, Y., Zhu, L., Du, X. & Guizani, N. Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach. *IEEE Netw.* **33**, 27–33 (2019).
4. Ryalat, M., ElMoaqet, H. & AlFaouri, M. Design of a smart factory based on cyber-physical systems and internet of things towards industry 4.0. *Appl. Sci.* **13**, 2156 (2023).
5. Shen, M. et al. Blockchain-assisted secure device authentication for cross-domain industrial iot. *IEEE J. Sel. Areas Commun.* **38**, 942–954 (2020).
6. Yang, T. *et al.* Secure and traceable multikey image retrieval in cloud-assisted internet of things. *IEEE Internet Things J.* (2024).
7. Awan, S. et al. Iot with blockchain: A futuristic approach in agriculture and food supply chain. *Wirel. Commun. Mob. Comput.* **2021**, 1–14 (2021).
8. Shen, M. et al. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. *IEEE J. Sel. Areas Commun.* **38**, 1229–1241 (2020).
9. Zhang, L., Li, F., Wang, P., Su, R. & Chi, Z. A blockchain-assisted massive iot data collection intelligent framework. *IEEE Internet Things J.* **9**, 14708–14722. https://doi.org/10.1109/JIOT.2021.3049674 (2022).
10. Mohanta, B. K. *et al.* Decauth: Decentralized authentication scheme for iot device using ethereum blockchain. In *TENCON 2019–2019 IEEE Region 10 Conference (TENCON)*, 558–563 (IEEE, 2019).
11. Mohanta, B. K. *et al.* Decauth: Decentralized authentication scheme for iot device using ethereum blockchain. In *TENCON 2019-2019 IEEE Region 10 Conference (TENCON)*, 558–563 (IEEE, 2019).
12. Panda, S. S. et al. Authentication and key management in distributed iot using blockchain technology. *IEEE Internet Things J.* **8**, 12947–12954 (2021).
13. Khalid, U. et al. A decentralized lightweight blockchain-based authentication mechanism for iot systems. *Clust. Comput.* **23**, 2067–2087 (2020).
14. Cachin, C. *et al.* Architecture of the hyperledger blockchain fabric. In *Workshop on distributed cryptocurrencies and consensus ledgers*, vol. 310, 1–4 (2016).
15. Choi, J., Cho, J., Kim, H. & Hyun, S. Towards secure and usable certificate-based authentication system using a secondary device for an industrial internet of things. *Appl. Sci.* **10**, 1962 (2020).
16. Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. & Ylianttila, M. Two-phase authentication protocol for wireless sensor networks in distributed iot applications. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, 2728–2733 (IEEE, 2014).
17. Malani, S., Srinivas, J., Das, A. K., Srinathan, K. & Jo, M. Certificate-based anonymous device access control scheme for iot environment. *IEEE Internet Things J.* **6**, 9762–9773 (2019).
18. Ni, J., Lin, X. & Shen, X. S. Efficient and secure service-oriented authentication supporting network slicing for 5g-enabled iot. *IEEE J. Sel. Areas Commun.* **36**, 644–657 (2018).
19. Hernandez-Ramos, J. L., Pawlowski, M. P., Jara, A. J., Skarmeta, A. F. & Ladid, L. Toward a lightweight authentication and authorization framework for smart objects. *IEEE J. Sel. Areas Commun.* **33**, 690–702 (2015).
20. Matsumoto, S. & Reischuk, R. M. Ikp: Turning a pki around with decentralized automated incentives. In *2017 IEEE Symposium on Security and Privacy (SP)*, 410–426 (IEEE, 2017).
21. Esfahani, A. et al. A lightweight authentication mechanism for m2m communications in industrial iot environment. *IEEE Internet Things J.* **6**, 288–296 (2017).
22. Lara, E., Aguilar, L., Sanchez, M. A. & García, J. A. Lightweight authentication protocol for m2m communications of resource-constrained devices in industrial internet of things. *Sensors* **20**, 501 (2020).

23. Lu, Y., Wang, D., Obaidat, M. S. & Vijayakumar, P. Edge-assisted intelligent device authentication in cyber-physical systems. *IEEE Internet Things J.* **10**, 3057–3070 (2022).
24. Nosouhi, M. R., Sood, K., Grobler, M. & Doss, R. Towards spoofing resistant next generation iot networks. *IEEE Trans. Inf. Forensics Secur.* **17**, 1669–1683 (2022).
25. Jan, M. A. et al. Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-cps. *IEEE Trans. Ind. Inf.* **17**, 5829–5839 (2020).
26. Jia, X., He, D., Kumar, N. & Choo, K.-K.R. Authenticated key agreement scheme for fog-driven iot healthcare system. *Wirel. Netw.* **25**, 4737–4750 (2019).
27. Li, X. et al. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Syst. J.* **14**, 39–50 (2019).
28. Ben Amor, A., Jebri, S., Abid, M. & Meddeb, A. A secure lightweight mutual authentication scheme in social industrial iot environment. *J. Supercomput.* 1–23 (2023).
29. Patel, C., Bashir, A. K., AlZubi, A. A. & Jhaveri, R. Ebake-se: A novel ecc-based authenticated key exchange between industrial iot devices using secure element. *Digit. Commun. Netw.* **9**, 358–366 (2023).
30. Dang, T. K., Pham, C. D. & Nguyen, T. L. A pragmatic elliptic curve cryptography-based extension for energy-efficient device-to-device communications in smart cities. *Sustain. Cities Soc.* **56**, 102097 (2020).
31. Cui, Z. et al. A hybrid blockchain-based identity authentication scheme for multi-wsn. *IEEE Trans. Serv. Comput.* **13**, 241–251 (2020).
32. Kumari, D., Kumar, P. & Prajapat, S. A blockchain assisted public auditing scheme for cloud-based digital twin healthcare services. *Clust. Comput.* **27**, 2593–2609 (2024).
33. Gautam, D. *et al.* Blockchain-assisted post-quantum privacy-preserving public auditing scheme to secure multimedia data in cloud storage. *Cluster Comput.* 1–14 (2024).
34. Prajapat, S. *et al.* Quantum secure authentication scheme for internet of medical things using blockchain. *IEEE Internet Things J.* (2024).
35. Gong, L., Alghazzawi, D. M. & Cheng, L. Bcot sentry: A blockchain-based identity authentication framework for iot devices. *Information* **12**, 203 (2021).
36. Panda, S. S., Satapathy, U., Mohanta, B. K., Jena, D. & Gountia, D. A blockchain based decentralized authentication framework for resource constrained iot devices. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–6 (IEEE, 2019).
37. Almadhoun, R., Kadadha, M., Alhemeiri, M., Alshehhi, M. & Salah, K. A user authentication scheme of iot devices using blockchain-enabled fog nodes. In *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, 1–8 (IEEE, 2018).

Acknowledgements
We acknowledge the efforts of the editor and the valuable comments of anonymous reviewers during the revision of this research.

Author contributions
Z.C. and X.W. contributed equally to the article, designed and developed the scheme, carried out the experiments, analyzed the results and drafted the manuscript. S.A. revised the manuscript. W.S. and S.H. supervised the scheme and revised the manuscript. All authors have read, and approved the manuscript.

Funding
This work was supported in part by National Key Research and Development Program of China under Grant 2021YFB2012300, the National Natural Science Foundation of China under Grant 62173101, the Basic and Applied Basic Research Funding of Guangdong Province under Grant 2022A1515011558 and Grant 2022A1515010865, the Guangzhou Science and Technology Funding under Grant 202201020217, the Key Laboratory of On-Chip Communication and Sensor Chip of Guangdong Higher Education Institutes under Grant 2023KSYS002.

Declarations

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to W.S. or S.H.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.