Distributed authentication scheme for Industry Internet Platform application based on consortium blockchain

Min Yan¹, Haibo Huang²,³, Shuaifeng Yang³*

¹ Trusted Computing and Information Assurance Laboratory, Institute of Software Chinese Academy of Sciences, Beijing, 100190, China
² Department of Economics and Management, Beijing University of Posts and Telecommunications, Beijing, 100876, China,
³ Department of Security Technology, China Industrial Control Systems Cyber Emergency Response Team, Beijing, 100040, China,
*Corresponding author’s e-mail: yanmin20@iscas.ac.cn

Abstract. With the rapid development of industrial internet services, the integration of IT/OT has enabled the continuous expansion of network security boundaries and put forward higher requirements for platform application cross-domain identity authentication. Aiming at the insufficient security of existing user-centric identity authentication schemes, this paper proposes a distributed authentication scheme based on the consortium blockchain in industrial Internet platform. The solution analyzes its applicability to the Industry Internet Platform from three perspectives: network architecture, industrial Internet platform user identity control, and user privacy. It defines the identity composed of consortium ID and consortium digital identity credentials, and builds distributed authentication architecture. The consortium blockchain is used to record the digital identity information of the industrial Internet platform users, and the consortium ID and the consortium digital identity credential are designed to realize the industrial Internet platform business securely access.

1. Introduction

Industry Internet Platform (IIP) business integrates cutting-edge technologies and promotes the rapid development of multiple new businesses. Each new business system is connected to a large number of terminals and the number of users continue to increase, making the IIP network security boundary continues to expand. Security risks such as unauthorized access to the access domain on the edge of the platform increased. As the first gateway to protect network security, the digital identity authentication system (DIAS) must not only meet the cross-domain unified identity authentication requirements of new businesses, but also deal with the problems and challenges brought about by cutting-edge technologies.

Aiming at the establishment of a unified and secure DIAS that adapts to new businesses, existing researches have proposed a "centralized--consortium--user centric" DIAS based on the degree of user control over digital identities. The traditional centralized DIAS based on public key infrastructure has problems such as poor interoperability of the identities of each centralized user, and the user’s identity data is completely managed and controlled by the centralized organization, but not controlled by the user. This will not only cause the user privacy leak, and hackers attacking the central authentication server will cause the entire authentication system to collapse[1].
As there are many security risks in centralized digital identities, consortium digital identities trusted by decentralized consortiums members have emerged. The consortium digital identities uses blockchain as the underlying technology of decentralization consensus trust, and establishes a set of distributed consortium ID that can be independently controlled by users. Users have their own digital identities and only allow specific permission organizations or individuals access, store, analyze or share identity data, which can be adapted to new business scenarios such as large-scale and widespread IIPs.

This article proposes a consortium blockchain-based decentralized DIAS architecture in IIP, gives the consortium member globally unique definition of distributed entity identity, and designs the entity consortium’s digital identity certificate functions.

2. Blockchain based decentralized DIAS

2.1. the applicability of blockchain technology

The identity authentication of the IIP system is based on digital identity. Due to changes in users' requirements for identity authentication or access control, it is gradually evolving from centralized digital identity, consortium digital identity, and user-centric digital identity to consortium decentralized identity system. The following describes the adaptability of the blockchain based distributed identity authentication technology in the IIP system from three perspectives: network architecture, user identity control, and privacy protection.

2.1.1. network architecture

Most systems in the IIP are distributed architectures. Adding a centralized identity authentication server to the distributed infrastructure poses certain security risks. For example, the centralized authentication server is vulnerable to DDOS attacks, single point of failure attacks, and vulnerability exploitation, which can easily lead to the leakage of normal user identity information and the consumption of server memory resources. In addition, once the central server is attacked, it will cause the entire identity authentication to fail and cause irreparable consequences, and the security is low.

The distributed architecture of blockchain technology fits the needs of distributed heterogeneous identity authentication of IIP systems. Many organizations in the IIP provide one or more independent peer nodes to build a trusted distributed identity authentication consortium network. Each consortium network node runs on different servers in different organizations. Compared with the traditional centralized authentication model, its nodes are scattered and decentralized, which can effectively defend against DDoS attacks. And when an attacker attacks a single node, even if the node fails, it will not affect the distributed authentication service of the entire consortium. At the same time, the distributed identity authentication of the blockchain consortium is implemented by all organizations in the trusted consortium network to jointly exercise the rights of consensus and accounting, thereby eliminating the dependence on the traditional single central authority identity authentication agency, and ensuring the multi-party storage traceability of data, and Anti-tampering[3].

2.1.2. user identity

Judging from the development trend of digital identity technology solutions in the existing IIP system, the user's own control requirements for identity information are showing a more refined trend. For example, the traditional centralized digital identity relies on an authoritative third-party organization, such as the core certificate authority CA of the public key infrastructure PKI. The authoritative third-party organization fully manages and controls the identity information of all users, and the organization owns the issued identity data. Complete control and interpretation rights; consortium digital identity user identity relies on several super identity centers, and users still cannot achieve self-identity control; user-centric digital identity is committed to achieving user complete control of identity and cross-domain transplantation, But the security is weak.
The blockchain stores credible information on the chain, and the entire chaining process is recorded in the blockchain distributed ledger. According to the automatic execution strategy of the smart contract, users can perform independent registration and management of their identities. Consortium distributed identity authentication based on blockchain can further refine the control granularity of user identity information, and ensure the traceability, tamper-proof, and high security of identity information records. In addition, blockchain technology can build a new architecture and collaboration model that builds an consortium trust system between institutions, individuals, and machines, builds a distributed consortium trust network, connects trusted data, and is recognized by various consortium organizations. The blockchain-based consortium identity can adapt to different decentralized identity authentication requirements according to different business scenarios, and provide a globally unique distributed entity identity and trusted data exchange protocol in the consortium, which can promote cross-departmental and cross-border Regional identity authentication and data cooperation.

2.1.3. privacy
If the user identity information in the IIP is scattered on various heterogeneous distributed systems, users cannot control related private data, which will result in the failure to protect personal privacy rights and cause privacy leakage. However, the existing digital identity technology form of the IIP system lacks the ability to provide reliable identity authentication while taking into account identity security and protecting user privacy.

Blockchain technology is highly integrated with privacy protection technologies such as homomorphic encryption and zero-knowledge proof. Through the multi-party consensus mechanism and the blockchain identity privacy protection mechanism, the sharing of data in the consortium network environment can not be tampered with, and the identity privacy information of the data is protected. Through homomorphic encryption technology, it supports the calculation of additive homomorphism and multiplicative homomorphism ciphertext homomorphism of data on the chain, and realizes the "calculated invisible" of data, thereby solving the problem of user identity information privacy. The privacy protection mechanism of distributed identity authentication based on blockchain can support the physical identity of entities and the storage of digital identity certificates under the chain. The entity minimizes or selectively discloses information to other institutions, and uses zero-knowledge proof to prevent any third-party reverse Infer the identity of the entity in the real world or other scene semantics.

As a result, the blockchain consortium trusts that the distributed identity authentication technology can fit and make up for the defects and problems faced by the current IIP identity authentication. The consortium trusts that distributed digital identities rely on blockchain technology to realize the full life cycle management of the digital identities of the entities in the IIP, as well as the secure interaction and access control between the entities, to ensure the credible storage of identity information after multi-party consensus, Traceable and tamper-proof. In addition, identity verification gets rid of the dependence on the traditional central authentication server, which can prevent the traditional IIP central authentication server from being attacked and the whole network authentication paralyzed.

2.2. Definition
Generally, the blockchain-based IIP distributed digital identity consists of two parts: the consortium distributed digital identity identifier (Consortium ID) and the consortium digital identity certificate (Consortium Cert). The Consortium ID is used to uniquely identify an entity within the consortium in the IIP. The essence of the Consortium Cert is a collection of identity attribute declarations associated with IIP entities.

2.2.1. Consortium ID
The Consortium ID is an identifier composed of a character string and a public-private key pair associated with it. It has the characteristics of being globally open and unique in the consortium, distributed, autonomous and controllable, and cross-chain reuse. The consortium ID is used to
uniquely identify an entity in the IIP. The entity can be an IIP system, equipment, regulatory department, IIP system upstream and downstream units, or external third parties (such as logistics agencies), etc. Each entity in the IIP can independently complete the registration, analysis, update or cancellation of the consortium ID.

Each entity in the IIP can have multiple digital identities at the same time. Each digital identity is assigned a unique consortium identity ID, which is suitable for different application scenarios, and has a one-to-one Consortium Cert corresponding to the consortium ID in different scenarios. The consortium ID and its public key information are stored on the consortium distributed identity ledger. For privacy protection considerations, there is no associated information between different identities, which can effectively avoid the collection of owner identity information in the IIP.

2.2.2. **Consortium Cert**

The identity ID of the consortium is disclosed globally within the consortium and does not include any content related to the real identity information of the IIP entity. Therefore, the identity of the IIP entity cannot be verified by the consortium identity ID alone. It must rely on the IIP entity's identity. Consortium Cert. Essentially, the core of the consortium's digital identity certificate is a collection of entity identity attributes, with the signature of the issuer and the metadata of the certificate attached.

Consortium digital identity credentials are used to describe certain identity attributes of certain entities in the IIP. The ID holders of each consortium in the IIP can prove to other entities that some of their attributes are trustworthy through the Consortium Cert. At the same time, the consortium's digital identity certificate is self-saved by the user and the data structure of the certificate is defined by the blockchain distributed ledger storage, combined with cryptographic technologies such as digital signature, homomorphic encryption and zero-knowledge proof, to protect all entities in the IIP The privacy of your identity is not violated.

1) **Data structure of Consortium Cert**

The data structure of the Consortium Cert includes three parts: Consortium Cert metadata, entity attribute collection, and relevant signature information of the Consortium Cert issuer. The metadata of the Consortium Cert includes the name of the certificate, certificate issuer, issuance date, etc.; the Consortium Cert issuer's signature information includes the signature algorithm used by the issuer, the creation time of the certificate, the creator, and digital signature information.

2) **过程 of Consortium Cert**

The digital identity certificate business includes three types of roles: Consortium Cert issuer, Consortium Cert holder, and Consortium Cert verifier. Before each issuer, holder and verifier carry out the business interaction of the Consortium Cert, they first register the corresponding consortium ID according to the business scenario requirements of the corresponding IIP and store it on the chain. Both parties of the business interaction must first complete the analysis and verification of the identity ID of the consortium of both parties to establish a trusted connection. Then, on the basis of this trusted connection, each issuer, holder, and verifier conduct business interaction based on consortium distributed identity credential verification.

Consortium Cert issuer refers to an entity that has user data and can issue digital identity certificates, such as IIP system business or regulatory authorities; Consortium Cert holders are physical users in the IIP, such as IIP systems or equipment, security management personnel, upstream and downstream units of the IIP system, external third-party organizations, etc. IIP users request the issuer of the Consortium Cert to issue the corresponding Consortium Cert, and present the Consortium Cert to the Consortium Cert verifier. The Consortium Cert issued by the issuer is only for self-preservation by IIP users, so that they can be used again in the future. The Consortium Cert verifier accepts the Consortium Cert and performs verification. If the verification is passed, it will provide users with a certain type of service. In addition, the distributed identity ledger of the consortium only maintains the database storing the distributed identity identifier of the consortium and the voucher definition of each consortium's digital identity certificate, and the data entity of each consortium's digital identity certificate is self-saved by the user.
In summary, each entity in the IIP obtains a unique distributed digital identity in the consortium domain by registering the Consortium ID and the Consortium Cert. At the same time, each entity performs the authentication of the Consortium Cert on the basis of the consortium identity ID to perform cross-domain business applications.

3. IIP Distributed Identity Authentication

3.1. Architecture

The overall components of the distributed certification system architecture are divided into basic layer, service layer and application layer. The basic layer is mainly composed of the organizations in the IIP system jointly building the underlying consortium distributed identity network, and each blockchain node jointly maintains the same consortium distributed identity ledger through a consensus mechanism. The ledger is used to store the User Consortium ID and its public key information, and the Consortium Cert definition.

The intermediate agent in the service layer receives the upper-layer user interface request and performs the actual business logic processing of the consortium digital identity. The consortium ID protocol provides the processing logic for the registration, verification, update, and cancellation of the single-chain or cross-chain globally unique consortium ID within the consortium. The Consortium Digital Identity Credentials Protocol provides the processing logic for the issuance, update, verification and revocation of digital identity certificates of IIP users. In addition, the service layer also provides users with reliable storage solutions for identity data according to different privacy protection strategies.

The application layer client is for IIP systems or IIP equipment, IIP system users or security managers, IIP business or regulatory departments, upstream and downstream units, and external third-party agencies to build applications to support users. The cycle management of the distributed digital identity of the consortium covers the issuance, verification, update, and revocation of the user consortium ID and credentials. At the same time, the application layer provides necessary application management services, including message notification, identity wallet and other services, where the identity wallet stores the user's consortium ID and identity credentials in various application scenarios.

3.2. Operating mechanism

The operation of the IIP system consortium distributed authentication system includes four levels of operation mechanisms: consortium ID generation, credential generation, Block generation and Consortium Cert verification.

consortium ID generation: each IIP system user registers the consortium identity ID and its public-private key pair, hashes it to generate an information digest and attaches it with a time stamp, and sends it to the consortium's distributed identity ledger after being digitally signed.

Consortium Cert definition and credential generation: The Consortium Cert issuer signs the data structure of the defined certificate and sends it to the ledger. After that, the issuer issues Consortium Certs for IIP system users based on the data structure of the digital identity certificate.

Block generation: The consortium blockchain network receives the identity ID of each user consortium and the definition of digital identity credentials, verifies the electronic signature, and if the verification is passed, a new block is generated and broadcast to the entire network, and a consensus is reached and written into the consortium distributed identity Ledger.

Consortium Cert verification: IIP system users first verify the consortium ID, then query the voucher definition on the ledger, verify the presented Consortium Cert information, and complete the verification of the user's identity.
3.3. Full life cycle management of consortium ID

3.3.1. Identity ID full life cycle management

First, according to the data structure definition of the consortium ID, various users of the IIP system register different consortium DIAS according to their own types (equipment/person/institution). The consortium ID has a fixed header ConsortiumID. Different users select the type of the corresponding ConsortiumID, generate a globally unique random string, and bind the corresponding public and private key pair at the same time. The user sends the consortium ID information to the consortium's distributed identity ledger to generate a block on-chain storage, and store it in the local identity wallet.

Secondly, the IIP system user uses the consortium ID and its private key, attaches a timestamp to digitally sign and sends a verification request, and the receiver analyzes the sender's consortium ID. Then, the receiver queries the sender's federated identity and the public key bound to it stored on the distributed identity ledger, and uses the public key information to verify the digital signature of the sender's federated identity.

In addition, when the user needs to update the consortium ID or public key information stored on the chain, the user sends a change request to the consortium identity service node, and the consortium ID is updated on the ledger after the verification of the ledger by the consortium network, and identifies The old consortium ID is not available, and the user ID wallet is updated simultaneously.

Finally, according to the user's demand for revoking the consortium ID, the user can submit a cancellation request, and after the consortium network queries the ledger for review, the corresponding consortium identity ID stored on the ledger is marked as revoked. In addition, the revoked consortiumID in the user identity wallet is set to a user unavailable state.

3.3.2. Consortium Cert full life cycle management

(1) Issuance of Consortium Certs

The credential issuer issues a consortium digital identity certificate to legitimate users. The consortium digital identity certificate means that the user is bound to the consortium digital identity certificate, and the user has the consortium digital identity certificate, which can obtain distributed trust in the entire system.

First, the user and the credential issuer verify the consortium ID and public key. If the verification is passed, the user sends a request for the credential to the credential issuer, and requests the consortium distributed identity ledger to obtain the definition of the Consortium Cert. The credential issuer receives the request and verifies the user. If the verification is passed, the credential issuer creates the user's Consortium Cert based on the definition of the Consortium Cert, and sends it to the user. The user accepts the Consortium Cert and stores it in the local identity wallet.

(2) Consortium Cert verification

The Consortium Cert verification process includes: first, the certificate owner and the certificate verifier verify the consortium ID and public key. If the verification is passed, the certificate owner will take out the issued certificate from the local identity wallet and distribute it to the consortium. The identity ledger requests the definition of consortium digital identity credentials. The credential owner creates a credential certification message and sends the credential certification message to the credential verifier. The voucher issuer receives the voucher certification message, requests the consortium distributed identity ledger to obtain the definition of the Consortium Cert, and verifies the Consortium Cert of the certificate owner. If the verification is passed, the certificate owner provides some subsequent types Service.

(3) Consortium Cert renewal and revocation

The update process of the consortium's digital identity certificate includes: First, the certificate issuer updates the consortium's digital identity certificate definition on the consortium's distributed identity ledger, and provides the certificate owner with a notification that the updated certificate can be issued. The certificate owner requests the blockchain consortium distributed identity ledger to obtain the updated definition of the consortium's digital identity certificate, and sends a request to update the
certificate to the certificate issuer. The credential issuer receives the update request and verifies the user. If the verification passes, the credential issuer updates the user's Consortium Cert based on the updated Consortium Cert definition, and sends it to the user. The user accepts the updated Consortium Cert and stores it in the local identity wallet.

In the revocation operation of the Consortium Cert, since the consortium digital identity definition contains the attribute of the Consortium Cert validity period, when the user's Consortium Cert reaches the validity period, it is regarded as the Consortium Cert revocation.

4. Conclusion
The paper proposes a consortium blockchain-based distributed authentication scheme, designs the consortium ID protocol and consortium cert protocol to realize the secure, and cross-domain identity authentication for users in the IIP. Compared with the traditional identity authentication system, this scheme realizes the secure sharing and autonomous control of identity data for users of the IIP, and has the advantages of decentralization, good scalability, and high security. In the next step, it will study the optimization and improvement methods of key technologies involved in the application process of the consortium distributed authentication in the IIP, and promote the combination of the alliance distributed authentication technology and the specific application scenarios of the IIP business.

References
[1] WANG Jing. Application of the Unified Identity Authentication and User Management Platform in Electric Group Enterprise[J].NETINFO SECURITY,2016(12):81-85.
[2] XIA Tongfei,QIN Hao,LI Zhi.Application and Research of Trusted Identity Authentication Cloud Service in Ubiquitous Power Internet of Things[J].Electric Power Information and Communication Technology,2019,17(07):11-15.
[3] WU Wei,WEI Xiao,WEI Shimin.Uniform identity authentication model based on mutually unreliable enterprise consortium[J].Computer Engineering and Design,2007(19):4634-4636.
[4] D. Recordon, D. Reed, OpenID 2.0: a platform for user centric identity management, in DIM ’06: Proceedings of the 2nd ACM Workshop on Digital Identity Management, 2006, pp. 11–16.
[5] ZHANG Lihua,HU Fangzhou,HUANG Yang.Identity Authentication Protocol of Micro-grid Power Based on Consortium blockchain[J].Journal of Applied Sciences,2020,38(01):173-183.
[6] CHEN Xiong,ZHU Yu,FENG Ke,YU Tongwei.Identity Authentication of Power System Safety and Stability Control Terminals Based on Blockchain[J].Journal of Guangxi Normal University (NATURAL SCIENCE EDITION),2020,38(02):8-18.
[7] KANG Chongqing, YAO Liangzhong. Key scientific issues and theoretical research framework for power systems with high proportion of renewable energy[J]. Automation of Electric Power Systems, 2017, 41(9): 2-11.
[8] ZHANG Lihua,HU Fangzhou,HUANG Yang.Identity Authentication Protocol of Micro-grid Power Based on Consortium blockchain[J].Journal of Applied Sciences,2020,38(01):173-183.
[9] MIRANBEIGI M, IMAN-EINI H. Hybrid modulation technique for grid-connected cascaded photovoltaic systems[J]. IEEE Transactions on Industrial Electronics, 2016, 63(12): 7843-7853.
[10] CAO Yijia, LI Qiang, TAN Yi, et al. A comprehensive review of Energy Internet: basic concept, operation and planning methods, and research prospects[J]. Journal of Modern Power Systems and Clean Energy, 2018, 6(3): 399-411.