A Blockchain-Enabled Trusted Identifier Co-Governance Architecture for the Industrial Internet of Things

Ru Huo, Shiqin Zeng, Yuhong Di, Xiangfeng Cheng, Tao Huang, F. Richard Yu, and Yunjie Liu

The authors provide a detailed introduction to IEEE 802.15.3d and the key design principles beyond the developed standard. They describe the target applications and usage scenarios, as well as the specifics of the IEEE 802.15.3d physical and medium access layers. They present the results of the initial performance evaluation of IEEE 802.15.3d wireless communications.

Abstract

Recently, the Industrial Internet of Things plays a vital role in the new round of technology innovation and industry competition, where the identity resolution system is its key component. However, there are some problems in the existing Handle-based identity resolution architecture. Therefore, a trusted identifier co-governance architecture is proposed, and a prototype system is designed and implemented in this article. Specifically, we design a blockchain-based decentralized framework for identifier service, identifier life cycle management based on smart contract, and a data storage mechanism for a trusted identifier. The whole architecture could solve the problems of single point of failure, data tampering, and governance deviation, and reduce the trust cost in the process of data circulation. The simulation results reveal that the system has achieved good results in terms of delay and throughput.

Introduction

The Internet has been rapidly developed during the past few decades, and there is a trend that consumer Internet is gradually turning to production-oriented Internet. One of the most important representatives of the production-oriented Internet is the Industrial Internet of Things (IIoT). It is supported by 5G and other information and communication technologies (ICTs) combined with intelligent machines, people, and materials [1]. Because of the huge improvement in productivity and economy that IIoT may bring, it has become the commanding height of global technology innovation and industry competition.

Identity resolution technology is the key to industrial digitization and the foundation of data circulation in IIoT. It provides a unified coding scheme, standard data structure, and complete methods of data acquisition and management. As the most widely used identity resolution technology, the Domain Name System (DNS) has limitations to meet the needs of IIoT because of its insufficient resolution dimension, centralization, and weak security [2]. Some researchers attempted to solve these problems by patching and clean slate. Kalodner *et al.* [3] proposed Namecoin to decentralize DNS and ensure data security with blockchain. Wang *et al.* [4] proposed the ConsortiumDNS with faster algorithms to achieve consensus of consortium blockchain. Liu *et al.* [5] proposed the Decentralization Domain Name System (DecDNS) with a two-layer model. Handle is a common distributed identity resolution technology independent of DNS, with multi-dimensional data.

However, the above technologies still cannot fully meet the needs of IIoT for single point of failure, data tampering, and governance deviation. In the scenario of IIoT, it is particularly important to ensure the safety of industrial production and data circulation, and the fair rights and credibility of multiple parties. It is necessary to design a novel identity resolution architecture to naturally support and achieve better decentralization and credibility for identity resolution technology in IIoT.

In this article, we devise a solution to identity resolution with the trusted identifier co-governance architecture (TICA), and the prototype system is designed and implemented. The main work includes designing the decentralized framework for identifier service, building the identifier life cycle management based on smart contract, and proposing the data storage mechanism for trusted identifier. Our architecture introduces the features of blockchain [6] to improve Handle-based identity resolution architecture and address single point of failure, data tampering, and governance deviation issues. Additionally, some ideas of TICA can provide solutions and inspiration for identity resolution and IIoT.

The rest of the article is organized as follows. First, we present previous works and introduce the related technologies. After giving technical challenges and design principles via analysis, we propose TICA and describe its structure and details. We present the experimental results and analysis. Open issues are discussed. Finally, we conclude and outline future work.

Related Research Work

AAS and Identifier Service in IIoT

IIoT provides interconnection between machines and information networks, and innovative solutions for other industries in saving operation costs and

Ru Huo is with the Beijing University of Technology, China. She is also with the Purple Mountain Laboratories, China; Shiqin Zeng is with Shenzhen Power Supply Bureau Co., Ltd, China; Yuhong Di and Xiangfeng Cheng are with the Beijing University of Technology, China; Tao Huang and Yunjie Liu are with Beijing University of Posts and Telecommunications, China; F. Richard Yu is with Carleton University, Canada.

Digital Object Identifier: 10.1109/MCOM.001.2100448

improving system reliability [7]. Digitization is one of the most important conditions for IIoT to show its potential. The concept of an asset administration shell (AAS) helps IIoT realize digitization better.

Typically, an objective such as a conveyor belt or tire could be named as an asset. The AAS, a virtual representation of the assets, provides the interface to implement data interactions. It has many beneficial functions, such as information integration, data control, orchestration [7], and plug-and-produce [9].

Identifier service can help AAS realize the functions mentioned above. Furthermore, establishing identifier service may become a priority of IIoT, and the reasons are as follows:

1. The identifier service provides the functions of identifier data acquisition, identifier registration, identity resolution, data processing, and modeling. It plays a vital role in data standardized encapsulation and addressing.
2. The distributed data integration function provided by the identifier service can better support the rich application ecology of the upper layer. Therefore, an equitable and secure identifier service has the potential to be used widely in industrial applications, such as lifecycle management, product traceability, and supply chain management.

With the steady advancing of IIoT, a framework about identity resolution system of industrial Internet is proposed as shown in Fig. 1 [10]. The framework mainly consists of the national top-level node, the second-level node, the enterprise node, and the recursive node. These nodes form a layered structure from top to bottom. The second-level nodes are the public nodes that provide industrial enterprises with the assigned identifier and functions of identifier registration and identity resolution. The recursive node is the key entry of industrial data resources, which needs to be compatible with different resolution protocols to complete the resolution processing and improve the performance via some technology (e.g., cache technology).

Identity Resolution Technologies

Different technologies, such as DNS, OID, Ecode, and UID, have their own characteristics, but none of them can fully meet the requirements of IIoT [2]. Due to the concept of digital objects, Handle could be a benefit for IIoT. It can better identify, manage, and obtain the multi-dimensional data of physical entities. Furthermore, Handle has the characteristics of device and platform independence, and is suitable for solving interoperability problems of heterogeneous data in cross-domain information interaction scenarios.

The Handle System has a two-layer service framework, as shown in Fig. 2. The upper layer is the GHR, and the lower layer is the LHS. Both GHR and LHS are composed of multiple sites. The sites provide specific services for GHR and LHS, and data synchronization is achieved between different sites that provide the same service. The server is the physical undertaker of the site. One or more servers jointly store data to implement specific functions of the identifier service provided by the site, such as writing, updating, deleting, and querying. Sometimes, to meet the data management needs of certain scenarios, such as product monitoring in IIoT [11], Handle may use multi-level LHS.

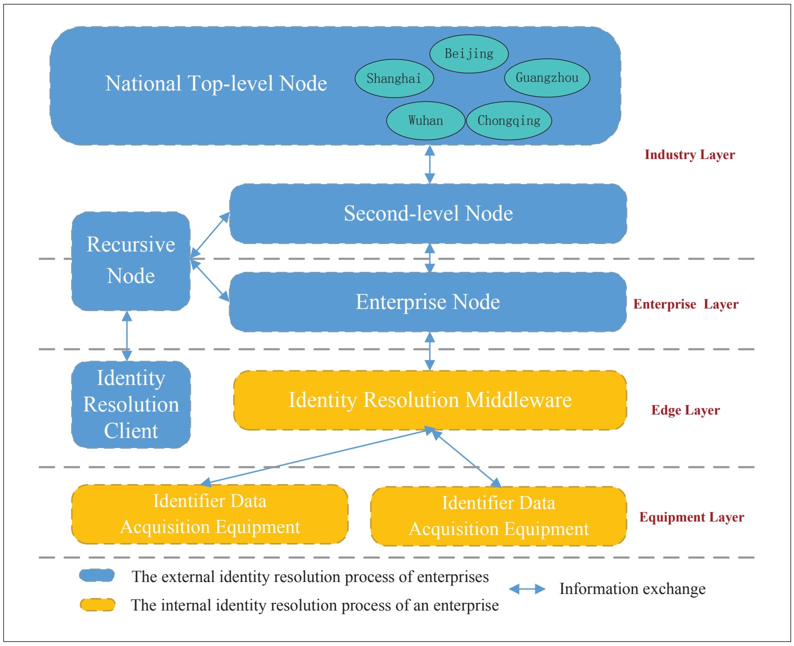
National Top-level Node
Beijing
Shanghai
Guangzhou
Wuhan
Chongqing
Industry Layer
Second-level Node
Recursive Node
Enterprise Node
Enterprise Layer
Identity Resolution Client
Identity Resolution Middleware
Edge Layer
Identifier Data Acquisition Equipment
Identifier Data Acquisition Equipment
Equipment Layer
The external identity resolution process of enterprises
The internal identity resolution process of an enterprise
Information exchange

FIGURE 1. The framework of the identity resolution system of Industrial Internet.

The Handle identifier consists of two parts: prefix and suffix. There are mainly two types of data in the Handle System, which are defined as follows.

1. *Authority Handle*: The data used to define the management relationship of the Handle service framework
2. *Common Handle*: The data used to identify and store digital objects for application

The prefix is managed by the GHR and is globally unique. The GHR maintains the identifier information of the prefix owner, and the LHS accesses the IP address by creating an Authority Handle. The suffix is managed by the LHS and is locally unique. The LHS provides resolution services for local Handle identifiers by creating a Common Handle, and creates an Authority Handle to manage subordinate prefixes, which could manage Handles under multiple prefixes, but Handles with the same prefix can only be managed by the fixed LHS.

Blockchain

Blockchain is generally considered to be a distributed ledger technology that evolves into a complete storage system based on logical control functions, such as smart contracts.

In our previous work, we presented a general hierarchical technical structure of blockchain and summarized its characteristics as decentralization, nontampering, openness, transparency, and contract autonomy [6]. Based on these characteristics, some papers have realized the integration of IIoT and blockchain. Liu *et al.* [12] proposed an anonymous reputation system based on blockchain to improve the credibility of IIoT-enabled retail marketing by preserving consumer privacy. Wu *et al.* [13] proposed an architecture that integrates blockchain and edge computing to solve the security and scalability of critical infrastructure in IIoT. Wang *et al.* [14] proposed an identity management protocol based on blockchain and a credit management framework to solve the problem of over-reliance on third parties. Also, some

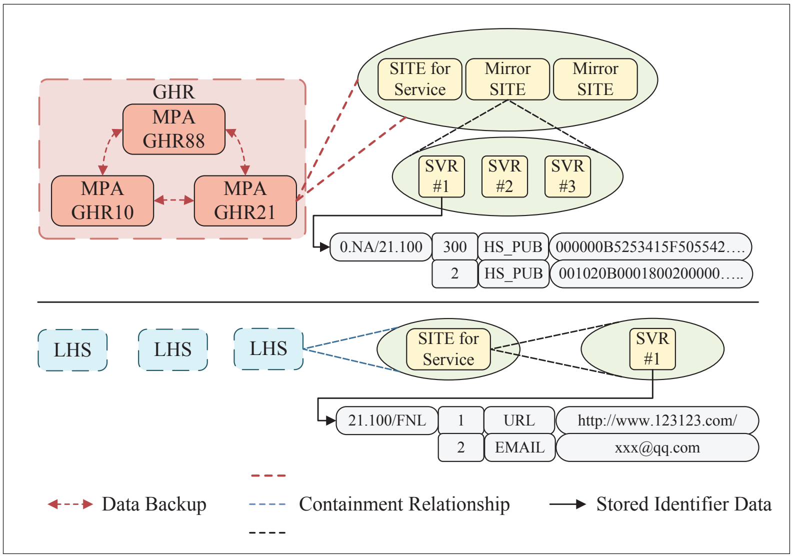

FIGURE 2. Service architecture of Handle.

works are devoted to solving the scalability issue and realizing quantum-resistant blockchain in the field of IIoT.

The Trusted Identifier Co-Governance Architecture

In order to solve some of the problems in the identity resolution system, this article proposes the TICA architecture. The main design goal is to combine blockchain and Handle technology in depth. It not only meets the needs of the object identifier and data acquisition, but also improves the data security and governance fairness of the identity resolution architecture.

Based on these considerations, the identity resolution architecture of IIoT should conform to the following design principles:

1. *Continuous service*: As for the single point of failure, the identity resolution architecture of IIoT needs to ensure the stability and availability of services in an open environment to prevent malicious attacks such as distributed denial of service (DDoS) causing interruption of identifier registration and resolution.
2. *Trusted data*: As for data tampering, the identity resolution architecture of IIoT should have data integrity verification and behavior traceability capabilities. It avoids the harmful effects of passive tampering, prevents enterprises from actively tampering with data, and reduces the trust cost of data interconnection.
3. *Decentralization*: As for governance deviation, the management behavior in the identity resolution architecture of IIoT should be open and transparent, which will increase the trust of enterprise nodes in second-level nodes and improve the enthusiasm for enterprise access.

Considering the above design principles, we propose TICA. The Handle-based TICA is based on a multi-level LHS structure and divided into three levels. The first level is the top-level node, which is maintained by some countries and responsible for managing the second level. The second level introduces blockchain and expands the second-level node into a second-level consortium blockchain network, which connects the top-level node and the enterprise node. It is maintained by different companies and organizations. The second level provides specific industries or multiple industries efficient and stable identity resolution service. The third level is the enterprise node, which is maintained by the enterprise and services inside. It not only protects data privacy of enterprises, but also makes the enterprises connect to the data resource pool of IIoT. Furthermore, the deployment type of enterprise node can be designed into three types, which are completely self-building, partially self-building, and full trusteeship.The identity resolution service of the enterprise is increasingly dependent on the second-level node.

The second-level node of TICA is composed of three parts, which are the decentralized framework for identifier service, the identifier life cycle management based on smart contract, and the data storage mechanism for trusted identifier. The three parts are shown on the right of Fig. 3, and some details can be seen on the left of Fig. 3.

The decentralized framework for identifier service is oriented to the second-level node scenarios for IIoT by drawing on the advantages of Handle's efficient layered service architecture and incorporating the decentralized working mechanism of blockchain. It defines multiple roles and establishes their management relationships, which improves the multi-level structure of LHS. The identifier life cycle management method defines the state transition rules of the Authority Handle and the Common Handle. It builds the resolution mechanism and management mechanism of the Handle service based on the smart contract. The trusted storage mechanism combines the distributed storage method of Handle and the distributed ledger technology of blockchain to design an identifier state ledger and the classified storage and synchronization methods.

Implementation Details of the Trusted Identifier Co-Governance Architecture

Based on the above design ideas and overall description of the framework, we introduce the specific implementation details.

Decentralized Framework for Identifier Service

The consortium blockchain network is composed of the second-level consortium node. Its trust foundation is constructed by the participants from the whole industry/regions, so it shows the characteristics of decentralization. There are three types of nodes in the second-level consortium node, which are the network management node (NMN), identifier service node (ISN), and enterprise registration node (ERN). The processes of block generation, consensus, and ledger maintenance are completed by designated members.

The NMN is responsible for the construction of the network, and monitoring the status of the network and each node. It is also the decision center for selecting the consensus algorithm of consortium blockchain.

The ISN is responsible for allocating the enterprise prefix (e.g., 88.100.1), and managing the Authority Handle of the enterprise prefix. It also provides external identity resolution service and public

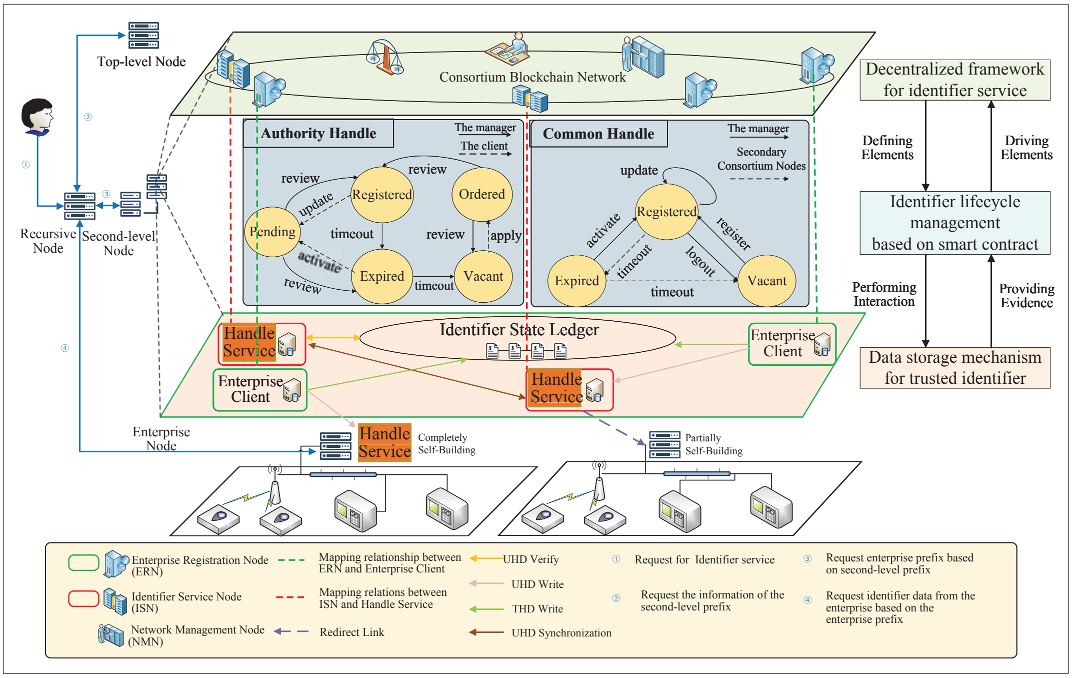
Top-level Node
①
②
③
④
Recursive Node
Second-level Node
Consortium Blockchain Network
Authority Handle
The manager
The client
review
update
Registered
Ordered
Pending
timeout
review
apply
activate
Expired
Vacant
review
timeout
Common Handle
The manager
Secondary Consortium Nodes
update
Registered
activate
register
timeout
logout
Expired
Vacant
timeout
Handle Service
Identifier State Ledger
Enterprise Client
Enterprise Client
Handle Service
Enterprise Node
Handle Service
Completely Self-Building
Partially Self-Building
Decentralized framework for identifier service
Defining Elements
Driving Elements
Identifier lifecycle management based on smart contract
Performing Interaction
Providing Evidence
Data storage mechanism for trusted identifier
Enterprise Registration Node (ERN)
Identifier Service Node (ISN)
Network Management Node (NMN)
Mapping relationship between ERN and Enterprise Client
Mapping relations between ISN and Handle Service
Redirect Link
UHD Verify
UHD Write
THD Write
UHD Synchronization
① Request for Identifier service
② Request the information of the second-level prefix
③ Request enterprise prefix based on second-level prefix
④ Request identifier data from the enterprise based on the enterprise prefix

FIGURE 3. The trusted identifier co-governance architecture.

service, such as review of identifier operation and traceability. The identifier data between ISNs are consistent. In addition, the ISN can provide enterprises with fully managed data storage services.

The ERN initiates various operations of data management for Common Handles under the enterprise prefix (e.g., 88.100.1/example), and participates in and supervises the life cycle of the enterprise Authority Handle (e.g., 0.NA/88.100.1). Furthermore, it can participate in trusted storage and integrity verification of specific data according to their own needs.

The workflow of the decentralized framework for identifier service is shown in Fig. 4. There are five roles in the framework: GHR administrator, top-level node administrator, NMN, ISN, and ERN. The relationship between all the roles is established by the multi-level structure of Handle.

The NMN is the owner of the second-level prefix and manages the consortium blockchain network. It can create identifiers under the second-level prefix, but cannot assign the enterprise prefix and verify the enterprise identifier. The ISN, created by the NMN, provides prefix allocation and identity resolution services for enterprises, so it is the identifier service provider of enterprises. The ERN is responsible for managing the Common Handle under the enterprise prefix. It needs to be authenticated by the ISN before it can be operated. In the second-level consortium blockchain network, the management process is completed by the participating nodes that follow the rules defined by the smart contract. The change and status data will be recorded in the ledger and supervised by all nodes.

Identifier Lif Cycle Management Based on Smart Contract

Domain name resolution systems (e.g., NameCoin and Blockstack), which are completely based on blockchain, realize autonomy by using smart contracts or scripting languages. Identifier life cycle management refers to the management of information and processes in the life cycle of Handle identifier data from prefix application, creation, update, cancellation, and prefix expiration by constructing state transition rules. In the identifier service framework based on decentralized LHS structure, the NMN, ISN, and ERN implement the multi-party co-governance of the Authority Handle and the Common Handle through the identifier life cycle management method. The second-level consortium node supervises the state change of the related Handle through the smart contract. It not only provides effective means of supervision, but also reduces the degree of centralization and avoids governance deviations.

The life cycles of different identifiers are managed by different roles. The roles are mainly divided into the manager, the client, and the

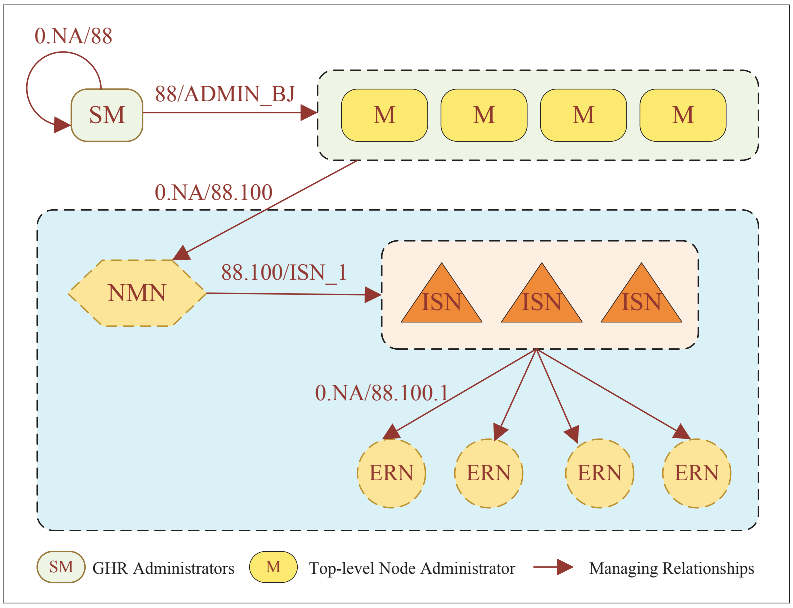

FIGURE 4. Decentralized framework for identifier service.

Identifier state management is the key to identifier life cycle management. The manager and the client have their own operation sets. These operations are recorded in the block, but the generated state alternation results are recorded in the identifier state ledger.

supervisor. The manager is responsible for modifying the content of Handle. It is assumed by the NMN, ISN, or ERN. The client can make a request for creation or update. It is assumed by the ISN or ERN. The supervisor is responsible for supervising the entire process that complies with pre-set rules to prevent governance deviations. It is assumed by the second-level consortium node.

Identifier state management is the key to identifier life cycle management. The manager and the client have their own operation sets. These operations are recorded in the block, but the generated state alternation results are recorded in the identifier state ledger. The state transition rules of Authority Handle and Common Handle are defined respectively:

1. *Authority Handle*: Figure 3 shows the state transfer rules of the Authority Handle. Authority Handle mainly has five states: Vacant, Ordered, Registered, Expired, and Pending.

   If an organization wants to become an identifier service node in the second-level consortium node, the organization first needs to apply for creating an administrator Handle, and submit the site public key, site information, and so on. The creation is completed after being reviewed by the network administrator. Before the administrator Handle expires, the identifier service node can apply for data modification, and the modification is completed after the network administrator confirms. The second-level consortium node specifies the use period of the Handle through the smart contract. After the use period expires, the administrator can make the Handle enter the expired state. If the activation application is not submitted within a certain period, the Handle will be cancelled and can be re-applied. Similarly, the enterprise prefix Authority Handle also needs to go through a similar management process.
2. *Common Handle*: Common Handle mainly has three states: vacant, registered, and expired. Figure 3 shows the state transfer rules of the Common Handle. Enterprises can create identifiers and update data by themselves. In a multi-organization data sharing scenario, companies can form a sharing contract for certain identifiers. When the timeout cannot be resolved, this function is linked to specific applications and is not discussed in detail in this article.

Data Storage Mechanism for Trusted Identifier

The process information of digital assets is recorded in the distributed ledger. Blockchain uses "block" and "chain" to describe the basic characteristics of the data structure in its distributed ledger. In the identity resolution system of IIoT, an account-based method is used to store identifier state data. The identifier state ledger records Handle state information.

- *Common Handle Storage Mechanism*: Although the blockchain can effectively prevent tampering and avoid single points of failure, there is a problem of high resource overhead. If all the identifier are stored in the identifier state ledger, the node will not be able to carry a huge amount of identifier data. Therefore, the mechanism classifies Handle data into Trusted Handle Data (THD) and Untrusted Handle Data (UHD). To avoid resource overhead and low efficiency, the credible data is stored in the identifier state ledger as a digital asset and the untrusted data is stored in the database of the identifier service node.

In the THD state ledger structure, the Handle identifier is key, and the value set includes THD data, UHD verification data, and so on. Figure 3 is a schematic diagram of the storage scheme for Common Handle data. The process mainly includes writing, synchronization, and verification.

First, the ERN initiates a service Handle registration request through the registration client. The registration client classifies the request and sends it to the identifier service node or the blockchain node.

Second, the ISN and ERN follow the Handle protocol to complete the authentication and UHD registration process. Nodes in the consortium blockchain network collect transactions, package them into blocks, and complete THD registration after the consensus accounting process.

Finally, UHD synchronization is performed between the databases of ISNs. ISNs can request integrity verification of synchronized UHD from the state ledger of the consortium blockchain network. If the verification fails, the identifier data will be marked as abnormal.

On one hand, this solution writes the verification information of THD and UHD into the distributed ledger from the beginning of registration, ensuring the data integrity of the Common Handle in the storage and synchronization process. On the other hand, writing key data into a distributed ledger can avoid the risk caused by the single point of failure and improve the availability of Common Handle data.

2. *Authority Handle Storage Method*: Authority Handle is the prerequisite for enterprises to verify administrator identity and manage the identifier, and is also a step that must be passed to resolve the Common Handle. Therefore, the second-level consortium node records all the Authority Handle data with the state ledger.

Figure 3 is a schematic diagram of the storage scheme for Authority Handle data. Participants of the second-level consortium nodes can read the ledger data and jointly supervise the changes of the Authority Handle data, but the write permissions of each node are different.

Specifically, the enterprise node has the authority to write the enterprise prefix Authority Handle data and manages the data together with the ISN according to a certain logic. The ISN manages all enterprise prefixes and has to write permission for all enterprise prefix Authority Handles. The NMN is responsible for managing ISNs, and it can modify their identifier verification information and write corresponding Authority Handle data.

This solution stores the Authority Handle data in the identifier state ledger, effectively preventing the authentication data and the key resolution data from being tampered with. The verification of corporate identifier is done through a blockchain network, avoiding availability damage caused by the single point of failure.

Experimental Results and Discussions

This section presents a simulation-based performance evaluation of TICA. Our framework is based on Hyperledger Fabric, and we set up two servers to simulate the basic nodes of it. We take our TICA (the experimental group) to compare with the traditional Handle-based architecture (the control group). The experimental group introduces blockchain to expand the second-level node into a consortium blockchain network to solve the legacy problems of Handle and improve performance. The results are as follows.

Error Rate

The throughput of resolution is defined as the maximum number of queries per second of the system. The response error rate under specific throughput is used for measuring the performance of the architecture. To ensure the high availability of the resolution service, the response error rate should be lower than 1 percent in theory. The test results are shown in Fig. 5. It shows that the response error rate increases with the increase of throughput. When the throughput is 23,000 times/min, the response error rate of the control group is about 1 percent. When the throughput is 24,000 times/min, the response error rate of the experimental group is about 1 percent. Under the same 1 percent error rate, the throughput of TICA is 1000 times/min higher than that of traditional architecture.

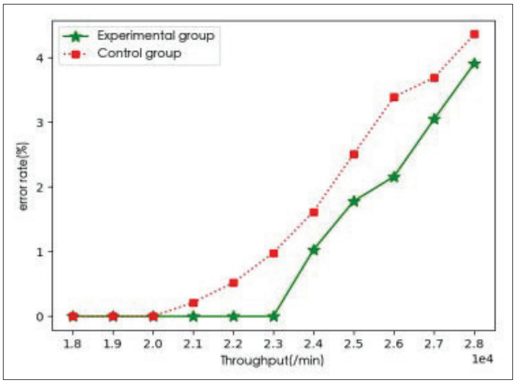

FIGURE 5. The result of the error rate test

Average Delay

The average delay is defined as the average time consumed by the system to complete the trusted resolution, which includes the time for resolution and verification. It measures the performance of the system when it provides the trusted resolution service. To minimize the error, 10 experiment repetitions between the experimental group and control group are performed. For resolution, the two groups have subequal delay, as it is mainly caused by the common Handle resolution cross-WAN. For verification, the delay of the experimental group is far lower than that of the control group due to the different verification mechanisms. The result is shown in Fig. 6. The reliable resolution performance of our architecture is increased by 37 percent on the premise of ensuring data security and co-governance fairness.

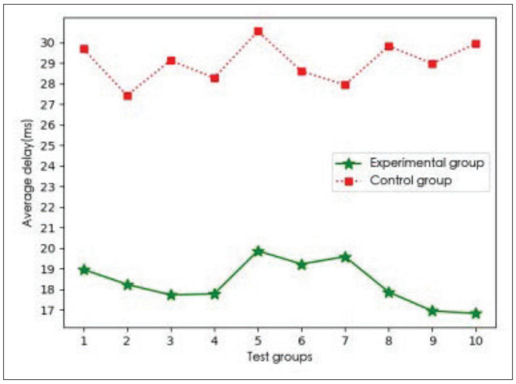

FIGURE 6. The result of the average delay test

The average delay is defined as the average time consumed by the system to complete the trusted resolution, which includes the time for resolution and verification. It measures the performance of the system when it provides the trusted resolution service. To minimize the error, ten repeated experiments between the experimental group and control group are performed.

The experimental results show that the proposed system could meet the concurrency requirements of traditional resolution and improve performance highly. Meanwhile, the nature-supported trusted resolution ensures not only better quality of experience, but also the safety and credibility of industrial production and data circulation. The system is particularly suitable for the scenario of multi-party governance in the industrial field.

Open Issues

This article proposes a trusted identifier co-governance architecture by leveraging blockchain technology and Handle technology. Although this article solves some problems in the security of identifier data and the fairness of governance, there are still some challenges that need to be adressed in future research:

1. The security, scalability, and decentralization of blockchain cannot be achieved at the same time. Therefore, a blockchain-enabled identity resolution system of IIoT needs to focus on the contradiction between transaction throughput and the speed of identifier generation, and between the limited capacity ledger and a large amount of identifier data on the premise of clear scene requirements. Also, it is possible to consider changing the structure of the chain and using quantum-resistant technology [15] to solve the above-mentioned problems in the blockchain.
2. Identity resolution is a prerequisite for data circulation in IIoT. Fine-grained access control for identifiers can comprehensively and effectively protect corporate data privacy. Therefore, identity access control based on attribute encryption technology will become a subsequent research direction.
3. AAS has two important goals, which are realizing the cross-industry data interaction and reducing the complexity of information filtering. Therefore, in follow-up work, we will also study using AAS for data modeling to achieve the integration of identity resolution.

Conclusions and Future Work

In this article, we have proposed a novel identifier co-governance architecture for IIoT. We also present the prototype implementation of this system. We have illustrated the feasibility and usability of the system. The experiments show that the proposed architecture has achieved better results in terms of error rate and average delay compared with the traditional Handle-based architecture. In the future, we hope to solve the impossible trinity of blockchain in our research and apply AAS to the identity resolution of IIoT. We will also research the identity access control based on attribute encryption technology.

Acknowledgments

This work was supported by the National Key Research and Development Program of Guangdong Province under Grant 2018B010113001, and in part by the MIIT of China 2020 (Identification Resource Search System for Industrial Internet of Things).

References

[1] H. Xu *et al.*, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," *IEEE Access*, vol. 6, 2018, pp. 78,238–59.

[2] Y. Ren *et al.*, "Potential Identity Resolution Systems for the Industrial Internet of Things: A Survey," *IEEE Commun. Surveys & Tutorials*, vol. 23, no. 1, 2021, pp. 391-430.

[3] H. Kalodner *et al.*, "An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design," *WEIS*, vol. 1, no. 1, June 2015, pp. 1–23.

[4] X. Wang *et al.*, "ConsortiumDNS: A Distributed Domain Name Service Based on Consortium Chain," *IEEE DSS*, 2017, pp. 617–20.

[5] J. Liu *et al.*, "A Data Storage Method Based on Blockchain for Decentralization DNS," *IEEE DSC*, July. 2018, pp. 189–96.

[6] S. Zeng *et al.*, "Survey of Blockchain: Principle, Progress and Application," *J. Commun.*, vol. 41, no. 1, Jan. 2020, pp. 134–51.

[7] P. Zhang, Y. Wu, and H. Zhu, "Open Ecosystem for Future Industrial Internet of Things (IIoT): Architecture and Application," *Csee J Power Energy*, vol. 6, no. 1, Sept. 2020, pp. 1–11.

[8] D. A. Bauer and J. Makio, "Hybrid Cloud - Architecture for Administration Shells with rami4.0 Using actor4j," July, 2019, pp. 79–86; http://dx.doi.org/10.1109/INDIN41052.2019.8972075, accessed Nov. 28, 2020.

[9] D. Lang *et al.*, "Pursuing the Vision of Industrie 4.0: Secure Plug-and-Produce by Means of the Asset Administration Shell and Blockchain Technology," *IEEE INDIN*, July. 2018, pp. 1092–97.

[10] Alliance of Industrial Internet, "Industrial Internet Architecture," Apr. 23, 2020; http://www.aii-alliance.org/bps/20200430/2063.html, accessed Nov. 28, 2020.

[11] M. Al-Bahri *et al.*, "Smart System Based on DOA and IoT for Products Monitoring Anti-Counterfeiting," *ICBDSC*, 2019.

[12] D. Liu *et al.*, "Anonymous Reputation System for IIoT-Enabled Retail Marketing ATOP POS Blockchain," *IEEE Trans Ind. Informatics*, vol. 15, no. 6, June 2019, pp. 3527–37.

[13] Y. Wu *et al.*, "Convergence of Blockchain and Edge Computing for Secure and Scalable IIoT Critical Infrastructures in Industry 4.0," *IEEE IoT Mag.*, vol. 8, Feb. 2019, pp. 2300–17.

[14] S. Wang *et al.*, "Eidm: a Ethereum-Based Cloud User Identity Management Protocol," *IEEE Access*, vol. 7, June 2021, pp. 115,281–91.

[15] S. Suhail *et al.*, "On the Role of Hash-Based Signatures in Quantum-Safe Internet of Things: Current Solutions and Future Directions," *IEEE IoT J.*, vol. 8, no. 1, Jan. 2021, pp. 1–17.

Biographies

Ru Huo (huoru@ bjut.edu.cn) received her B.S. degree in electronics and information engineering from Harbin Engineering University, Heilongjiang, China, in 2011, and her Ph.D. degree in information and communication engineering from Beijing University of Posts and Telecommunications (BUPT), China. From September 2015 to September 2016, she studied at the University of British Columbia, Vancouver, Canada, as a visiting Ph.D. student. She is currently a lecturer at Beijing University of Technology. Her current research interests include Industrial Internet of things, future networks, blockchain, and resource scheduling.

Shiqin Zeng is an engineer with the Shenzhen Power Supply Company. His current research interests include blockchain and Industrial Internet of things.

Yuhong Di is pursuing a Master's degree at Beijing University of Technology. Her research interests include blockchain, machine learning and Industrial Internet of Things.

Xiangfeng Cheng is pursuing a Master's degree at the Beijing University of Technology. Her research interests include blockchain, machine learning and the Industrial Internet of Things.

Tao Huang received his B.S. degree in communication engineering from Nankai University, Tianjin, China, in 2002, and his M.S. and Ph.D. degrees in communication and information systems from BUPT in 2004 and 2007, respectively. He is currently a professor at BUPT. His current research interests include future network architecture, software-defined networking, and network virtualization.

F. Richard Yu [F] is a professor at Carleton University, Canada. His research interests include connected/autonomous vehicles, artificial intelligence, cybersecurity, and wireless systems. He has received several professional awards, including the Ontario Early Researcher Award, Carleton Research Achievement Awards, and several Best Paper Awards from some first-tier conferences. He is a Fellow of the Canadian Academy of Engineering (CAE), Engineering Institute of Canada (EIC), and IET. He is a Distinguished Lecturer of IEEE in both VTS and ComSoc.

YunJie Liu received his B.S. degree in technical physics from Peking University, Beijing, China, in 1968. He is currently an Academician of the China Academy of Engineering, Chief of the Science and Technology Committee of China Unicom, and Dean of the School of Information and Communication Engineering, BUPT. His research interests include next generation networks, and network architecture and management.