Research on Industrial Internet Security Emergency Management Framework Based on Blockchain: Take China as an Example

Haibo Huang[1,2], Yuxi Gao[2](✉), Min Yan[3], and Xiaofan Zhang[2]

[1] Beijing University of Posts and Telecommunications, Beijing 100876, China
poehuang1@163.com

[2] China Industrial Control Systems Cyber Security Response Team, Beijing 100040, China
gemmagao@126.com

[3] Institute of Software, Chinese Academy of Sciences, Beijing 100093, China

Abstract. Building a national unified ISEMS (industrial internet security emergency management system) plays an important role in industrial cybersecurity defense. However, due to technical and management constraints, the current ISEMS has problems such as scattered security organizations, poor sharing channels, and fails to form an overall security guarantee capability for threat reporting, analyzing, warning, and disposing. The blockchain technology has the characters of decentralized trust construction, inter-organizational data sharing, data integrity assurance, data traceability, which just meets the requirements of the emergency management process. This paper analyzes the situation and challenges of ISEMS, describes the system architecture and organizational structure based on the blockchain, and describes the key implementation processes of blockchain-based ISEMS, including threat report, risk analysis, warning release and emergency response.

Keywords: Industrial cybersecurity · Emergency management · Consortium blockchain

1 Introduction

With the rapid development of global information technology and the deep reform of industrial structure adjustment, China's industrialization and informatization have deepened continuously, and the Industrial Internet has developed rapidly. According to statistics from the MIIT (Ministry of Industry and Information Technology), there are more than 50 Industrial Internet platforms having certain industrial and regional influences by 2019, some of which connected to more than 100,000 industrial equipment. With the rapid development of the industry, security threats are intensified increasingly, and Industrial Internet security events such as supply chain attacks, ransomware attacks, and

This work was financially supported by the National Key Research and Development Program of China (2018YFB2100400).

W. Lu et al. (Eds.): CNCERT 2020, CCIS 1299, pp. 71–85, 2020.
https://doi.org/10.1007/978-981-33-4922-3_6

data leaks are exposed frequently. Meanwhile, China's ISEMS management framework lacks the systematic design. Therefore, it is necessary to construct a comprehensive and secure emergency response mechanism and take closed-loop defense measures to active defense, real-time sensing, and emergency recovery. Building a national unified emergency management system is an important part of the Industrial Internet security defense. It comprehensively analyzes threat information through technology and management methods, builds capabilities such as early warning, notification, emergency handling, and information sharing, also helps emergency department dispatch resources, investigate risk, dispose emergency, to maintain the security of Industrial Internet platforms, networks, controls, equipment, and data.

However, owing to the scattered industrial internet emergency management institutions, the inconsistent sharing channels, and the insufficient risk analysis of the industrial internet infrastructure, it is hard to form a global security capability. The blockchain, which combining data blocks into a "chain" structure in chronological order uses distributed accounting, peer-to-peer communication, cryptographic technology, consensus mechanisms, and the disclosure of intelligent contracts to achieve a decentralized and tamper-proofing data storage [1], and can solve problems such as scattered institutions, unreliable data sources, and inability to achieve multi-party storage in industrial internet emergency management. It also well meets the needs of transparent and credible requirements in multiple parties during the emergency information management process.

2 Situation and Challenge

2.1 Organizational Structure

Seen from the Fig. 1, China's industrial internet emergency organization is a tree management structure. The root node is the national industrial internet security authority, mainly responsible for the emergency management function including early warning, risk notification, emergency response, information sharing, etc. Secondary nodes are provincial industrial internet security authorities and state-owned enterprises, which responsible for performing its management supervisors. Security vendors and scientific research institutes are also secondary nodes, responsible for reporting risk information and conducting risk research and emergency response. The third-level nodes are mainly city-level emergency management departments, small security vendors and research institutions, of which the function is consistent with the secondary node, and local industrial enterprises which are the main bodies in carrying out the disposal of risk and incident.

In recent years, the MIIT has continuously invested special funds to support the construction of industrial internet threat information sharing and emergency response command platform, through which the country can effectively improve the ability of grasping risk information, carrying out emergency command and response, nevertheless, it has not yet formed a nationwide ISEMS with vertical linkage and horizontal communication.

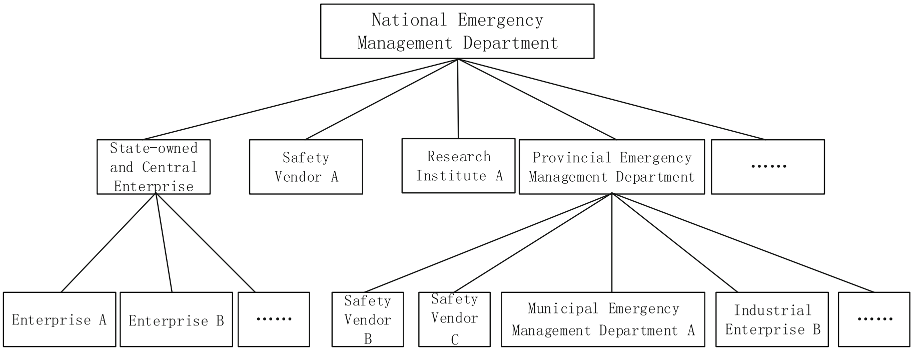
National Emergency Management Department
State-owned and Central Enterprise
Safety Vendor A
Research Institute A
Provincial Emergency Management Department
……
Enterprise A
Enterprise B
……
Safety Vendor B
Safety Vendor C
Municipal Emergency Management Department A
Industrial Enterprise B
……

Fig. 1. Management structure of China's ISEMS

2.2 Technical Status

Related Work. In terms of ISEMS research, Zhang Zhen et al. [2] analyzed the content and characteristics of the U.S. cybersecurity emergency management system, and made suggestions on the construction of China's cybersecurity emergency management system from the legal system, organizational structure, and operating mechanism. The establishment of command systems with incident response, information sharing, and emergency response from the technical level has not been further studied. Liu Feng [3], Zhao Xu et al. [4] proposed technical solutions to the provincial cybersecurity emergency management platform from the aspects of security access design, basic data collection, and command function implementation, but still lacking of consideration on information sharing, multi-party coordination, mutual identity trust, regulatory review, etc. Li Ruoyu et al. [5] established an emergency response system model for governments and enterprises, and pointed out the indispensability of security service vendors in national cybersecurity emergency response work, but did not give specific implementation plans at the operational and technical levels. Since 2003, the U.S. Department of Homeland Security has implemented continuous monitoring, early warning and response to Internet export threats of government agencies through the Einstein Plan. However, due to compatibility and diverse issues, only 68.7% of government agencies have achieved the goals of the Einstein Project by 2019 [6].

Problems. The problems in the construction of national ISEMS as follows.

1. Isolated islands of information. The communication among the information systems of institutions and organizations is incomplete. In the early stage of the big data era, the isolated information island problem is common in various industries and fields [7, 8]. Due to historical reasons such as insufficient top-level design and system performance constraints, the governments, security vendors and industrial enterprises have built independent threat information databases, vulnerability databases and emergency disposal systems, leading to an obvious "data chimney" effect, which comprehensively restricts the work efficiency of threat submission, sharing, and emergency disposal, etc.

2. Poor threat sharing. The security subject of Industrial Internet has weak willingness to share threat information. On the one hand, due to the high sharing frequency and complex path of industrial internet security data, data leakage may occur in the transmission process or non-legal endpoints; On the other hand, industrial internet security information has its own particular characteristics such as being multi-sourced, heterogeneous and distributed. Data classify measures are deficient to ensure the rationality of the scope of information sharing. In addition, for which the current information sharing rights and responsibilities are not clear and the audit tracking ability is insufficient, both leads to the enterprises unwilling to share information as "private property", and the competent authorities of industry are afraid of compulsory sharing.
3. Untrusted data source. Phishing, extortion, mining, etc. have become an important threat to Industrial Internet Security [9, 10]. In addition to directly attacking industrial enterprises, due to the lack of effective authentication and security measures for information source and transmission, hackers utilize the defects of insufficient end-user's management ability to spread malicious code embedded in risk information through industrial internet security emergency, causing a more targeted large-scale attack on competent authorities of industry and enterprises.
4. Inefficient emergency response. China has not yet established a unified emergency disposal command and communication system. The disposal of major cybersecurity incidents still stays in traditional ways such as SMS and telephone. It is difficult to meet the requirements in timeliness, portability, confidentiality, and other aspects. In addition, due to the lack of recognized evaluation methods, the security technology team cannot get the point in the first time after the security incident and hardly obtain evidence and division of responsibilities. With the combination of above two analysis, the repetitive emergency work has been carried out continuously.
5. Lack of motivation. As the main body of information reporting and emergency response, security vendors play an indispensable role in the emergency system, also the key to the effective implementation of the national industrial Internet security emergency. It is difficult to ensure the sustainability simply with the incentive measures of social responsibility. More effective measures must be introduced to improve the positivity of security vendors.
6. System security factors. The national ISEMS is intricacy while enormous system, with large cyber-attack surface and high security risk. Once centralized data storage infrastructure being attacked may lead to the collapse of the whole system. Meanwhile, with complex and multi-subject end-user identity, the ineffective management of all users results in the system vulnerability.

2.3 Challenge

In view of the issues above, the construction of national ISEMS has the following challenge.

1. Unified interface standard. The construction of a unified standard system interface and protocol could realize the interconnection of emergency information, form an emergency coordination and disposal mechanism with timely response and feedback.

which could provide channels for central and local emergency institute and organization to obtain and convey emergency information, realize the interconnection of emergency information systems of superior and subordinate units.

2. Confidentiality, availability and non-repudiation. Traditional information systems are vulnerable to single point of failure due to centralization. Through multi centralized storage deployment Enhance the robustness and usability of the system. In addition, by verifying the identity legitimacy and rationality of the users, the data source can be trusted, managed and traceable. Third, ensure the security of data transmission, storage and sharing, especially the integrity confidentiality and of data.
3. User incentive. In the process of information report and emergency disposal involving security vendors and scientific research institutions, the competitive ranking mechanism can improve the enthusiasm of participation, grasp the technical strength of each unit, so that an appropriate emergency response team could be found timely and accurately in a security incident. Second, for the industry competent departments and industrial enterprises, introduce the reward-punishment and assessment mechanism combined with national laws and industry regulations, implement the responsibility, and ensure the sustainable development of the ISEIMS.
4. Data classification. The system should store all kinds of data information, including system vulnerabilities, early warning notifications, typical cases, knowledge base, etc. In order to ensure the security and controllability of the data as a strategic resource, Data classify and grade according to its ownership, application scope, sensitivity and other dimensions, so as to improve the sharing and circulation of data use while protecting user privacy, realize the effective balance of data privacy and social utility.

3 Overview of Blockchain

3.1 Principle

Blockchain technology is a distributed ledger technology that uses the linked data structure to verify, store, generate, update data and ensure its transmission security. It is an integrated application and innovative combination of existing technologies such as distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm, etc. [11]. Its most significant technical feature is to change the centralization to decentralization, as shown in Fig. 2.

3.2 Research Status

Blockchain has the technical advantages of decentralization, non-tampering, traceability, high reliability and high availability, began to form distributed collaboration architecture supporting various typical industries [12]. According to the degree of openness, blockchain can be divided into three types: Public Blockchain, Private Blockchain and Consortium Blockchain. Public blockchain is completely decentralized, and also, any user can join the network, access and write data. The typical representatives are bitcoin and Ethereum. Private Blockchain is partial decentralized, and also, only part of users

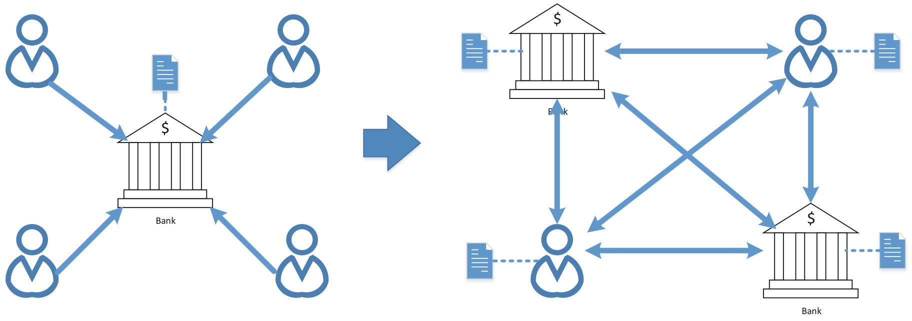

Fig. 2. Centralization and decentralization

can access, read and write data with internal permissions. Consortium Blockchain is multi centralized, and only authorized organizations can join the network. Its organization nodes are fully trusted and strongly scalable. Its scale could rise from institutional enterprises to the national level [13].

With the gradual development of blockchain, the research on its key technologies has shown multiple development directions, Herrera joancommarti [14], Saxena [15] do research on privacy protection issues such as anonymity and hybrid protocol of Bitcoin. Kishigami [16] and others proposed a blockchain-based digital content publishing system to move blockchain technology from theory to practice with intelligent contracts. Paul [17] and others calculated and verified the bitcoin mining energy consumption scheme, and studied the resource loss of blockchain technology. Mougayar [18] and others analyzed the trend of bitcoin vulnerability and countermeasures to study blockchain security technology. In addition, SANA, bjabendu, Jian Chen and others studied the application, management, security and openness of blockchain technology in the Internet of things, big data and other new fields [19–21].

4 Consortium-Blockchain-Based ISEMS

4.1 Base Model

The earliest form of blockchain is public blockchain, but the public blockchain is completely decentralized and difficult to supervise, which is different from China's governance structure. Consortium Blockchain is a form of "supervision friendly" blockchain, which is easy to pass the access system and use contract automation supervision to meet regulatory needs. Generally, the industry is oriented to institutions and enterprises, which need to solve the trust problems among them, and require the organizations that set up the blockchain to conduct identity authentication. The number of members in the blockchain can be controlled, and the characteristics of the Consortium Blockchain fully meet these needs. The Consortium Blockchain adopts the federal access mechanism with certain trust premise, which has a large space in the selection of efficient consensus algorithm and is easy to find a balance between security and performance. In recent years, various industries are actively exploring the "blockchain +" industry application mode. Based on the blockchain as a service (BaaS), the rapid construction of blockchain network and the implementation of industry application are gradually deepened. By deeply combining blockchain technology with cloud computing, BaaS platform integrates the underlying computing resources, blockchain service functions and upper business functions through the centralized management, realizes the available and dynamic expansion of the underlying blockchain framework with virtualization container, support the ability of multi-user, multi-chain, shared storage, log monitoring, etc., and greatly reduces blockchain barriers.

In this scheme, the Hyperledger Fabric Consortium Blockchain is proposed as the technology selection to design the ISEMS architecture. Fabric is the most widely used project in the hyper ledger blockchain open source project, aiming to promote the cross-industry application of blockchain, and its architecture model is shown in Fig. 3. Fabric Consortium Blockchain network is composed of members, which refers to the organization, also composed of several organizations with cooperative relationship. The users in the Consortium Blockchain belong to the members of the blockchain, which can be divided into two types, administrator and ordinary user. Administrator is the manager of blockchain, who can choose to join, exit the chain and install the intelligent contract. The user is the initiator of the transaction, and can interact with the blockchain network through the client or SDK. The nodes in the Consortium Blockchain refer to the physical resources actually running in the Consortium Blockchain. Each member of the blockchain has one or more peer peers and Ca nodes. Peer node is the node that each member can realize ledger storage, which includes endorsement node, bookkeeping node and master node. Endorsement refers to the process that a specific peer node executes a series of transactions and verifies their validity, and returns a successful or failed endorsement response to the members who generate the transaction proposal. The function of Ca node is to provide members in Fabric network with identity information based on digital certificate. The order node is jointly owned by the members of the blockchain. It is mainly responsible for collecting and sorting the received transactions of protection endorsement signature, generating blocks in sequence and broadcasting the transactions, in order to ensure that the nodes in the same chain receive the same messages and have the same logical order.

In the process of ISEIM, the organization is scattered and diverse. Based on the Consortium Blockchain, it can solve the problems, such as the organization is not mutual trust, the data source is not credible, not achieving multi-party storage, etc.

4.2 Architecture

The technical architecture of the ISEMS is shown in Fig. 4, which includes the underlying infrastructure, the intermediate service layer, and the calling API provided by the upper application system. In order to quickly start the consortium blockchain, the basic underlying blockchain framework uses the Swarm or K8s group management technology and container management technology to build the Fabric blockchain network framework, and automatically starts and manages the CA and peer nodes for blockchain members. The blockchain service layer management includes five modules of basic services, contract management, security management, operation monitoring, and query engines. Among them, the basic service module implements storage management, pluggable consensus mechanism, and network communication services. The contract management

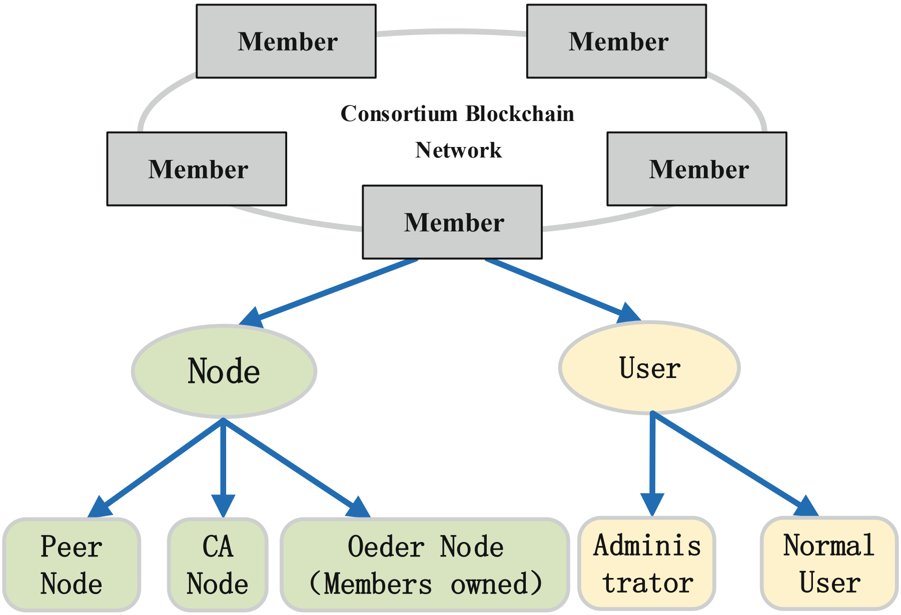

Fig. 3. Consortium blockchain network architecture model

module implements intelligent installation, operation, and version management. The security management module implements security mechanisms such as data encryption, access control, and multi-chain isolation. Core modules, such as operation monitoring and query engines, provide basic services for upper data API and blockchain service API interfaces. The blockchain API layer provides blockchain transaction read-write API, chain and contract management API, access control API and encryption authentication API, etc. It provides call interfaces for application requirements such as upper-level risk reporting, early warning release, information sharing, and emergency disposal.

4.3 Organization Structure

Organizational Structure of ISEMS based on consortium Blockchain is shown in Fig. 5. In the business scenario of ISEIM, the organization nodes involved are not completely parallel in function positioning. For example, local emergency management departments are responsible for reviewing the risk and vulnerability information reported by the regional security vendors, industrial enterprises and research institutions, and reporting to the central authorities only after passing the review. Therefore, for ISEIM business is multi-level and needs timely supervision, this scheme combines multi-chain and cross-chain technology to build multi-level consortium blockchain. Details can be seen in Fig. 5. The first-level members are composed of national and provincial industrial internet security emergency management department, security enterprises, state-owned enterprises and central enterprises. The second-level members are composed of provincial and municipal industrial internet security emergency management department, security

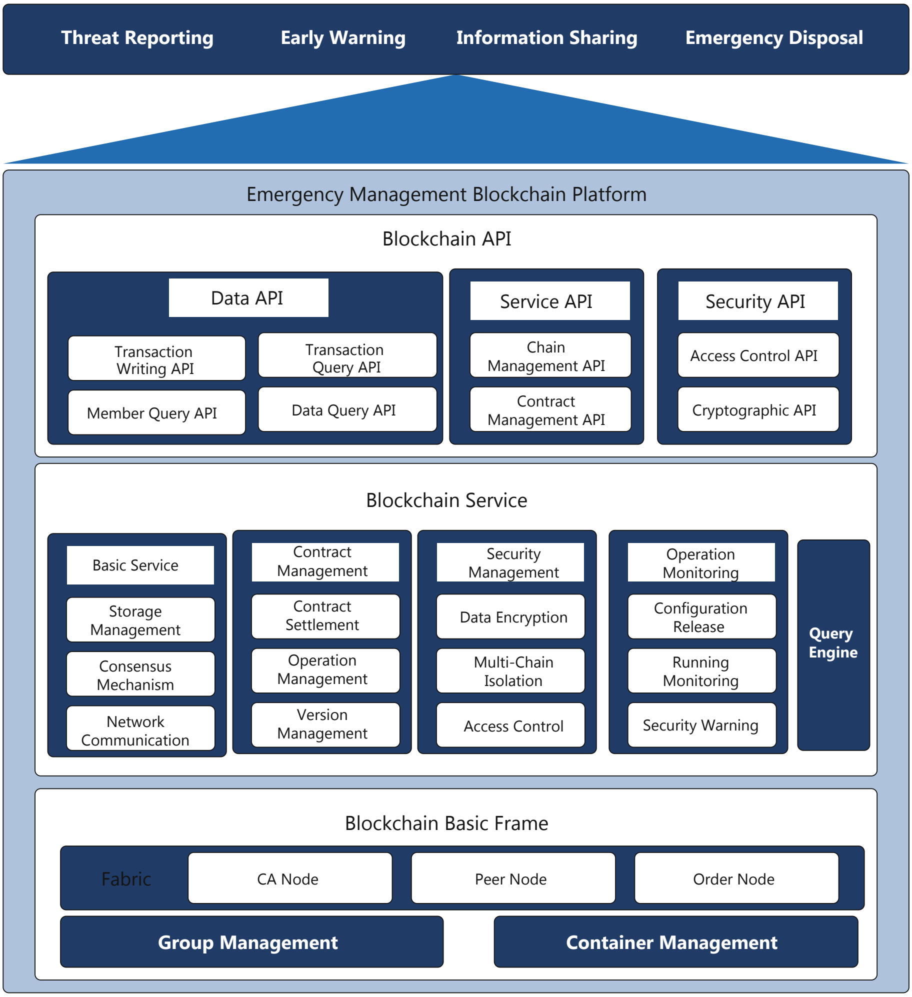

Fig. 4. Technical framework of ISEMS based on consortium blockchain

vendors, research institutions, etc. The provincial and municipal departments exist in both the first level and the second level. Each member of the primary and secondary consortium blockchain has its own administrator and ordinary user group. The administrator is responsible for consortium blockchain management, contract management and other functions. The subordinate local organization can set multiple users to report risks, receive early warnings and dispose emergencies. The administrator of national industrial internet security emergency management department is also responsible for blockchain management and contract management. Different users can respectively call intelligent contracts to implement information sharing, emergency strategy release, early warning, etc. For the local industrial Internet security emergency management departments, it is also necessary to create multiple users for risk reporting, information receiving, reviewing and releasing.

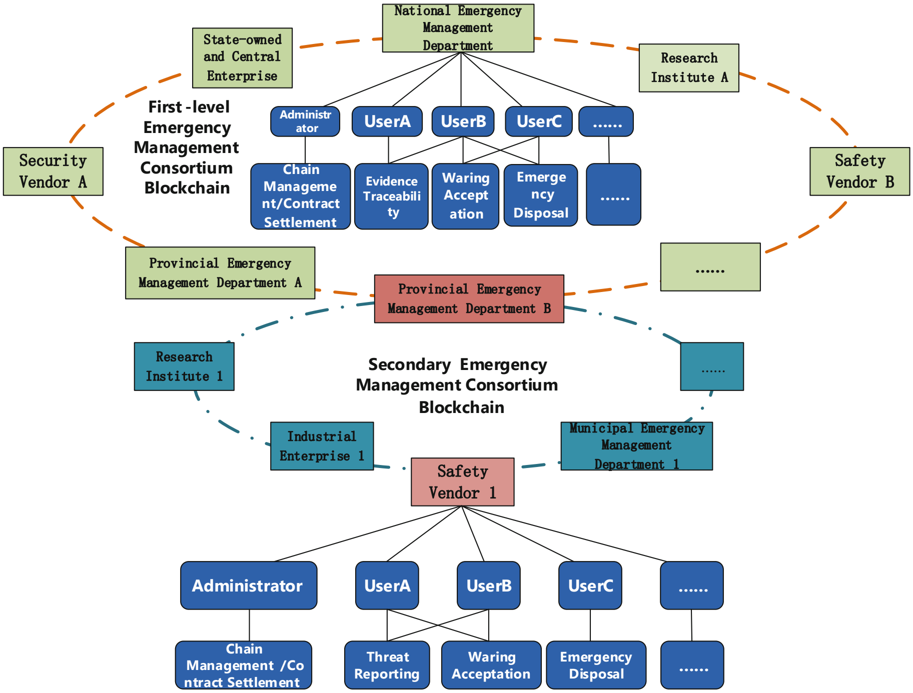
National Emergency Management Department
State-owned and Central Enterprise
Research Institute A
First-level Emergency Management Consortium Blockchain
Administrator
UserA
UserB
UserC
......
Security Vendor A
Safety Vendor B
Chain Management/Contract Settlement
Evidence Traceability
Waring Acceptation
Emergency Disposal
......
Provincial Emergency Management Department A
Provincial Emergency Management Department B
......
Research Institute 1
Secondary Emergency Management Consortium Blockchain
......
Industrial Enterprise 1
Municipal Emergency Management Department 1
Safety Vendor 1
Administrator
UserA
UserB
UserC
......
Chain Management /Contract Settlement
Threat Reporting
Waring Acceptation
Emergency Disposal
......

Fig. 5. Organizational structure of ISEMS based on consortium blockchain

4.4 Critical Process

Threat Reporting. The threat reporting process is generally handled by members of the secondary consortium blockchain such as local security vendors, research institutions and industrial enterprises. As shown in Fig. 6, after the consortium members find the vulnerability, Threat reporting subsystem call the blockchain smart contract through the risk reporting API to write the risk data to blockchain ledger. At the same time, according to the agreement in the endorsement strategy of the intelligent contract, they first submit it to the default endorsement node, i.e. the local emergency management department for review. After the review is passed, the risk information will be written into the ledger and synchronized to the members of the secondary consortium blockchain. In addition, the local emergency management department will submit the risk information to the first-level consortium blockchain and synchronously submit to the central emergency management department and other local emergency management departments for information sharing, so as to complete the reporting of emergency information under abnormal conditions. Compared with the traditional risk threat reporting process, the blockchain-based reporting, using the tamper-proof capability of the blockchain, can spread and synchronize to the peer timely.

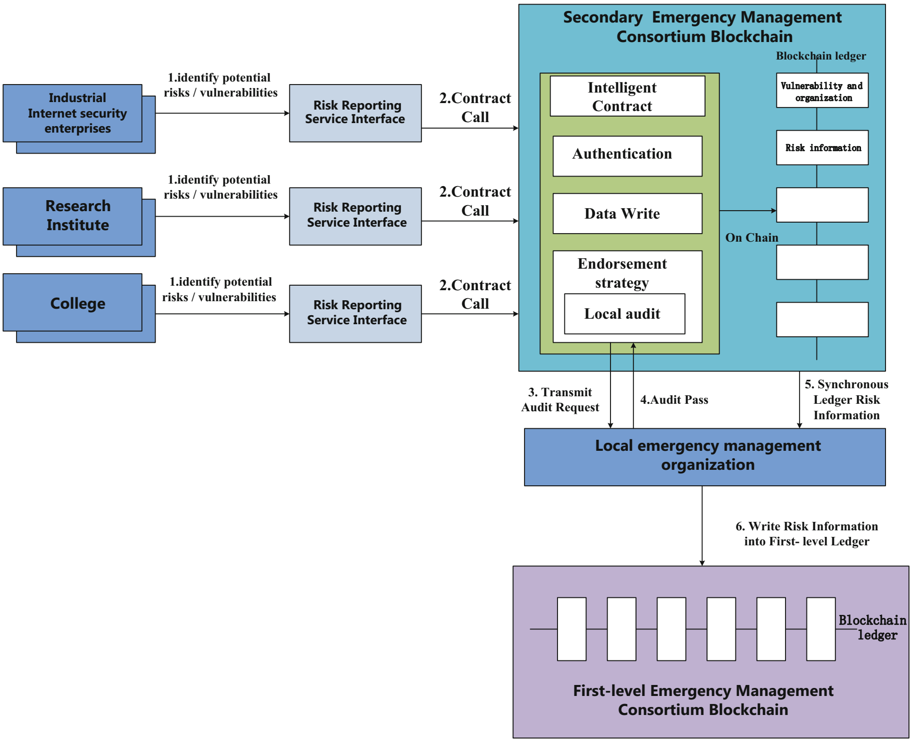
Secondary Emergency Management Consortium Blockchain
Blockchain ledger
Industrial Internet security enterprises
1.identify potential risks / vulnerabilities
Risk Reporting Service Interface
2.Contract Call
Research Institute
College
Intelligent Contract
Authentication
Data Write
Endorsement strategy
Local audit
Vulnerability and organization
Risk information
On Chain
3. Transmit Audit Request
4.Audit Pass
5. Synchronous Ledger Risk Information
Local emergency management organization
6. Write Risk Information into First- level Ledger
Blockchain ledger
First-level Emergency Management Consortium Blockchain

Fig. 6. Threat reporting process based on blockchain

Risk Analysis. The traditional risk analysis requires the central emergency management department to collect related risk data and organize relevant experts to carry out risk analysis and prediction. However, the risk analysis source data is too scattered to mobilize these resources to carry out analysis in time. The distributed blockchain-based risk analysis can realize risk vulnerability analysis and the training of distributed shared risk model locally. The online incremental learning of monitoring data is realized by capturing the data characteristics of each participant. Finally, each node can synchronize the updated risk model parameters or gradients to improve the risk prediction accuracy, as shown in Fig. 7.

Warning Release. When industrial internet security emergency event occurs, the early warning release and sharing system can quickly release vulnerabilities, notifications and policies to local competent departments or enterprises at all levels. In order to share emergency event knowledge base to specific members, and ensure members' identity trusted, the consortium blockchain firstly implements the identity authentication of members. Based on the CA digital certificate mechanism, it realizes the identification and authority

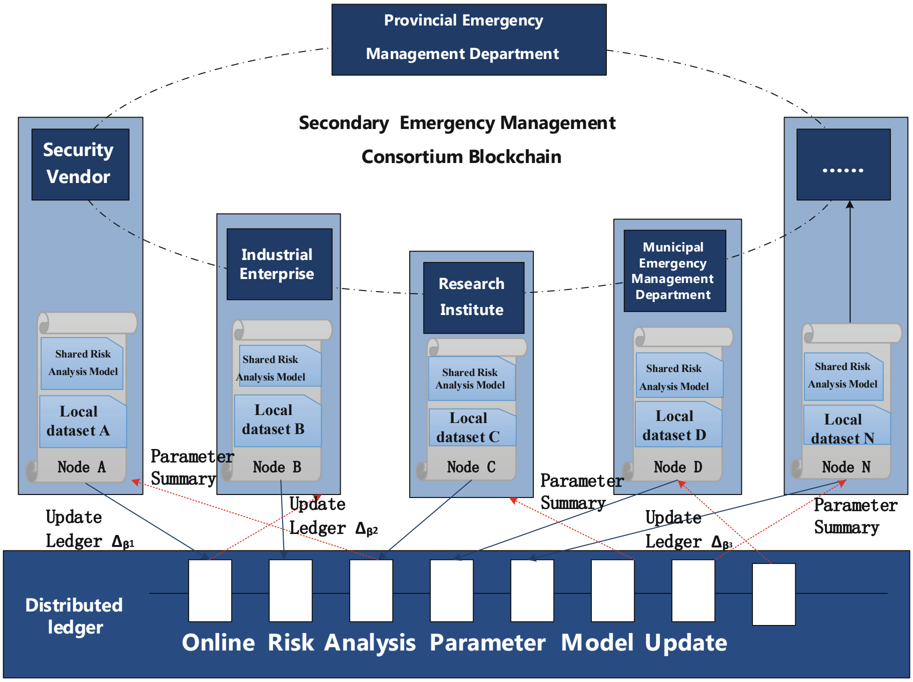
Provincial Emergency Management Department
Secondary Emergency Management Consortium Blockchain
Security Vendor
Industrial Enterprise
Research Institute
Municipal Emergency Management Department
......
Shared Risk Analysis Model
Local dataset A
Node A
Shared Risk Analysis Model
Local dataset B
Node B
Shared Risk Analysis Model
Local dataset C
Node C
Shared Risk Analysis Model
Local dataset D
Node D
Shared Risk Analysis Model
Local dataset N
Node N
Parameter Summary
Parameter Summary
Parameter Summary
Update Ledger Δβ1
Update Ledger Δβ2
Update Ledger Δβ3
Distributed ledger
Online Risk Analysis Parameter Model Update

Fig. 7. Risk analysis process based on blockchain

control for members, so that early warning can be managed and controlled. Secondly, based on the consortium blockchain, the parallel uplink authority management supporting the complex business among multiple organizations is implemented, as shown in Fig. 8. By building different sub chains in the consortium blockchain and assigning different roles to its members, the authority control of the sub chain management and the ledger data reading and writing is carried out, so that the early warning information can be updated in time and synchronized to the relevant organizations, the scope of the early warning release is controlled, and the access of the non-authorized organizations to the relevant information is prevented.

Emergency Response. Emergency response mainly includes evidence collection, tracing and coordination. traditional methods take a lot of valuable time to find the responsible person and technical support. Meanwhile, it is unable to quickly locate whether the support has good technical reserves in this risk field. In order to mobilize the enthusiasm of various organizations in ISEM and maintain the normal operation of the emergency management blockchain platform, a competition incentive mechanism is introduced to reward enterprises that can timely report vulnerabilities and analysis results. Through the scoring mechanism in blockchain, Management department can independently select security vendors or research institutions with higher score to support offline emergency response, and timely assist industrial enterprises in upgrading the system and vulnerability database. Detailed incentive model is referred in Fig. 9.

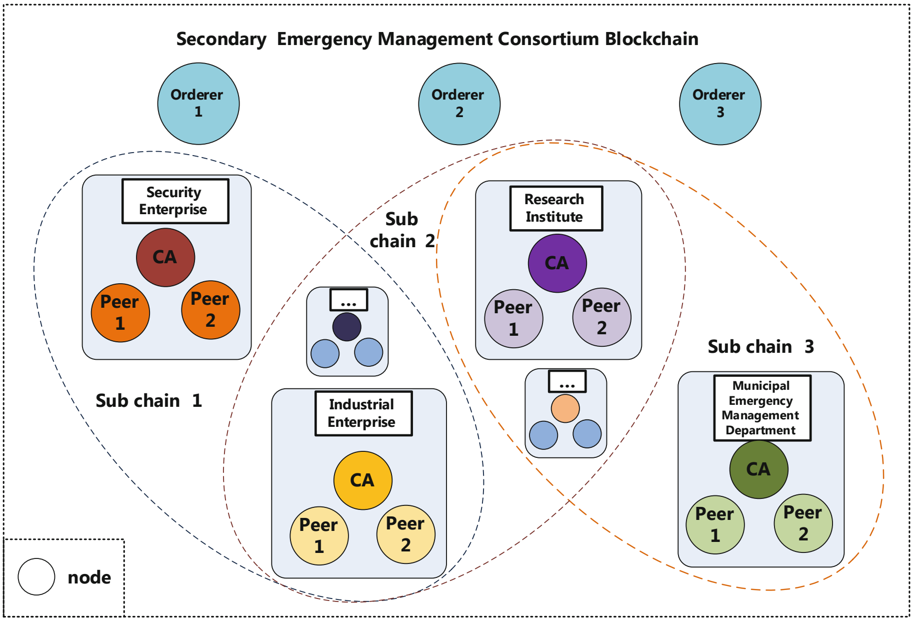

Fig. 8. Multi-organization sub chain division structure

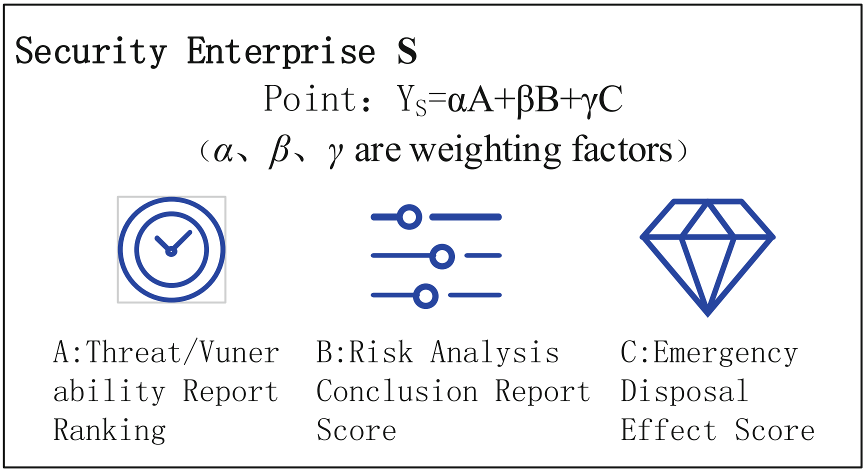
Security Enterprise S
Point： $Y_S=\alpha A+\beta B+\gamma C$
（α、β、γ are weighting factors）
A:Threat/Vunerability Report Ranking
B:Risk Analysis Conclusion Report Score
C:Emergency Disposal Effect Score

Fig. 9. User bonus point model

First of all, the report time of risk and vulnerability can be recorded on the blockchain ledger. Local emergency management organizations utilize the untampered and untraceable characteristics of blockchain to accurately and fast trace and rate the enterprise who report risk. Secondly, each organization can adjust the accuracy of the risk prediction model according to the local risk source data, improve the analysis model with adjusted accuracy. The institutions report the trained risk prediction model in time will be rewarded with points. Third, when the emergency management organization assigns the emergency assistance tasks, enterprises with high points and outstanding technical advantages will have the priority. Industrial enterprises can also score on the chain for the effect of support organizations' disposal, and the score results will be distributed to support enterprises in the form of points. The points will ultimately affect the industry influence of enterprises, provide basis for national projects, awards and honor declaration, and form a benign incentive for enterprises and research institutions to actively report, analyze and deal with safety risks.

5 Summary and Prospect

This paper analyzes the situation and challenges of ISEMS, including organizational structure and technical status. Meanwhile, the principle and situation of blockchain and the challenge of building consortium-blockchain-based ISEMS are briefly introduced. Besides, this paper describes the system architecture and base model of the ISEIM based on the blockchain, and describes the key blockchain-based implementation processes, including threat report, risk analysis, warning release and emergency response. In the future, we can further study the balance between the realization of enterprise data privacy and the enhancement of data's social utility based on blockchain technology, so that it could expand the upper application and play effectiveness in the fields of data classification, classification and sharing.

References

1. China blockchain technology and Industry Development Forum. White paper on China blockchain technology and application development. Department of information technology and software services, Ministry of industry and information technology (2016)
2. Zhang, Z., Sun, B., Li, B.: The US cybersecurity emergency management system and its enlightenment. Intell. J. (3), 94–98105 (2018)
3. Liu, F.: Cybersecurity situation awareness and emergency response platform solutions. Inf. Technol. Stand. **405**(09), 18–20 (2018)
4. Zhao, X., Wen, J.: Research on provincial cybersecurity emergency management platform based on security access design. Laboratory Research and Exploration, vol. 37, no. 268 (06), pp. 300–303 (2018)
5. Li, R., Jia, R.: Research on cybersecurity emergency response system. Network Security Technology and Application, p. 2 (2019)
6. Zhang, X., Xiao, Y.: Overview of the construction of cyberspace situational awareness, early warning and protection system in the United States and Its Enlightenment to China. Confidential Science and Technology, no. 67(04), pp. 22–28 (2016)
7. Wu, H.: Research on the information sharing mechanism of Chinese government in the era of big data (2017)
8. Kang, K.: Analysis of isolated information island in the field of e-government (2016)
9. Abhishek, G., Alagan, A., Glaucio, C.: Prevailing and emerging cyber threats and security practices in IoT-Enabled smart grids: a survey. J. Netw. Comput. Appl. **132**, 118–148 (2019)
10. Shi, Y.: Research on security defense technology of IT/OT integration in industrial internet environment. Inf. Technol. Netw. Secur. **38**(7), 1–5 (2019)

11. Zhou, P., Tang, X., Li, B.: Research Report on China's blockchain technology and application development. China blockchain technology and Industry Development Forum (2018)
12. Yang, L., Zhang, C., Wang, F.: Overview of blockchain technology research and application. Contemp. Econ. **4**, 126–128 (2018)
13. Zhang, S., Yang, Y.: Block chain technology foundation and application. Inf. Secur. Res. **4** 33(06), 89–94 (2018)
14. Herrera-Joancomartí, J.: Research and challenges on bitcoin anonymity. In: Garcia-Alfaro, J., et al. (eds.) DPM/QASA/SETOP -2014. LNCS, vol. 8872, pp. 3–16. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-17016-9_1
15. Saxena, A., Misra, J., Dhar, A.: Increasing Anonymity in Bitcoin (2014)
16. Kishigami, J., Fujimura, S., Watanabe, H., et al.: The blockchain-based digital content distribution system. In: 2015 IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud). IEEE (2015)
17. Paul, G., Sarkar, P., Mukherjee, S.: Towards a more democratic mining in bitcoins. In: International Conference on Information Systems Security (2014)
18. Mougayar, W.: Why Fragmentation Threatens the Promise of Blockchain Identity (2016). https://www.coindesk.com/fragment-blockchain-identity-market
19. Sana, M., Ahmad, K., Zanab, S.: Securing IoTs in distributed blockchain: analysis, requirements and open issues. Future Gener. Comput. Syst. **100**, 325–343 (2019)
20. Bhabendu, K.M., Debasish, J., Soumyashree, S.P.: Blockchain technology: a survey on applications and security privacy challenges. Internet Things **8**, 100107 (2019)
21. Chen, J., Lv, Z., Song, H.: Design of personnel big data management system based on blockchain. Future Gener. Comput. Syst. **101**, 1122–1129 (2019)