An Information Grading and Assessment Management System Based on a Dual Authentication Mechanism of Function and Management

Siwei Li[1], Chunzhi Meng[*], Hushuang Zeng[3], Xuexia Quan[4], Songyao Feng[5]

[1] wymfySWL@126.com, *vipwymfya@126.com, [3] wymfyhsz@126.com, [4] wymfyxxq@126.com, [5] wymfysyf@126.com

Information Communication Branch of Guangxi Grid Company, 530012, Nanning, China

Abstract. Starting from the perspective of cyberspace security management, this paper targets the organizational management needs in cyberspace security. In designing the hierarchical management architecture and authentication process for the public cyberspace infrastructure, the concept of partitioned system management is proposed. The overall architecture adopts a partitioned and layered design in which the core area, public area, and open area are divided. A dual authentication vulnerability management mechanism of both function and management is designed, providing security policies and implementation suggestions for user authentication and access control.

Keywords: Assessment Management System, Authentication Mechanism, Management System

1 Introduction

With the rapid development of network technology and the active participation of various objects in online communication practices, cyberspace has become a new form of social space, attracting widespread public attention. Overall, cyberspace in essence is a digital manifestation of the physical social space, which is formed by the interactions of different social forces [1].

Ref. [2] provides a comprehensive definition of cyberspace, stating that it is a global dynamic domain that creates, stores, adjusts, exchanges, shares, extracts, uses, and removes information and dispersed material resources. In China's National Key Research and Development Program *Cyberspace Surveying and Mapping*, cyberspace is defined as an artificial space built on the information and communication infrastructure, supporting various real-world activities related to information and communication technology [3].

Some Chinese scholars have proposed that cyberspace is the sum of elements such as carriers, information, and subjects. Therefore, cyberspace resources not only include the physical resources of the internet such as communication infrastructure and application support systems, but also contain the virtual resources such as content and user information on those physical facilities [4,5]. Fang Binxing further divides the constituents of cyberspace into four types: carriers, information, subjects, and operations. In summary, the resources and constituents of cyberspace mainly include carriers, information, subjects, and operations (e.g., creation, storage, adjustment, exchange, sharing, extraction, use, and), which have promoting effects on the

BDEDM 2024, January 12-14, Ningbo, People's Republic of China

DOI 10.4108/eai.12-1-2024.2347232

physical social space. The compositions of cyberspace are summarized in Fig. 1.

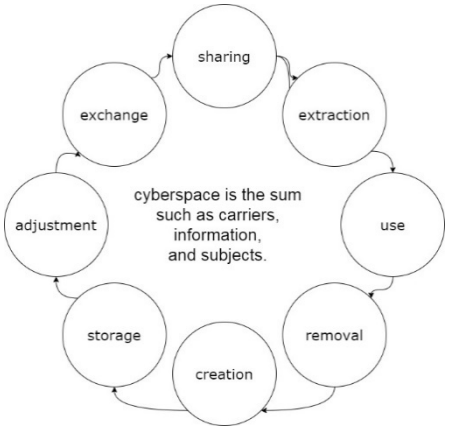

Figure 1. The compositions of cyberspace.

2 Key technologies for cyberspace security

The rapid development of the global Internet of Things (IoT) has posed challenges to myriad fields of network security.

One particularly pronounced issue is the security of IoT devices and applications. The operations and applications of myriad IoT devices generate massive privacy data, necessitating the defence against attacks on heterogeneous networks and demanding reasonable security control mechanisms. Specifically, in terms of IoT security access and control, it is pointed out that a series of security issues may arise during the transition from the Internet to the IoT, with an emphasis on the ubiquitous resource access control problems. In this context, security countermeasures include encryption and secret key management, perception layer authentication, secure routing, and access control mechanisms [7]. Researchers have investigated the means of authentication and evaluation to address IoT security issues such as the sensor node's susceptibility to attacks. At present, research on IoT security authentication and access control includes level-to-level management of network objects and hierarchical authentication based on network identity [8].

On the other hand, critical information infrastructure is deemed an essential part of network infrastructure for a nation, so its security has received widespread attention globally. Various countries have proposed development strategies and included the critical information infrastructure in the coverage of the highest-level security protection.

Therefore, it has gradually become a major network object management method to apply hierarchical classification and implement hierarchical management of network identity credibility and service providers. In the system framework of influencing factors for smart city's information security risk as proposed by Zou Kai *et al.* [9], urban information security is analyzed according to environmental, logical, and organizational dimensions. Focusing on the classification of network objects and access activities, the organizational dimension proposes examples of classification levels for organizational objects and specifies that management of

permissions and activities should vary for the various levels.

The International Electrotechnical Commission of the International Organization for Standardization (ISO/IEC) commenced research on network identity management earlier and attempted to standardize the trust levels of identity management from a risk perspective. They have successively released standards such as the *Entity Authentication Assurance Framework* [10] and *Identity Proofing* [11]. These standards target the identity management needs in e-commerce and other activities, with a focus on managing during identity authentication the credibility of processing procedures, management activities, and technologies related to physical identity. The credibility of identity is divided into three levels (high, medium, and low), and four levels of entity authentication assurance are specified (levels one, two, three, and four). The prominent feature of the ISO/IEC network identity management scheme is that it targets not only traditional network users such as people and organizations, but also new IoT elements of devices, software, and applications. In addition, countries such as the United States and the United Kingdom have successively released national strategies for identity management and authentication needs in e-government management activities. Asian states have also formulated relevant standards and specifications for authentication services in e-commerce and government activities based on electronic signature technology. The implementation results of these actors are listed in Table 1.

Table 1. Network user classification management situation.

state organization	application area	main contents and elements	managed object
ISO/TEC	electronic trading activities in the commercial field	the credibility of the identity and authentication process is divided	equipment organization user
EU and its member states	business and public services	the credibility of the identity and authentication process is divided	user object
Korea Japan	e-commerce and government affairs	division of the types and effectiveness of electronic signatures	user
USA	e-commerce	the credibility of identity and the security risks of division	organization user
UK	e-commerce	credibility of identity	object user
China	e-commerce, business and public services	risk division in the process of identity service	organization user

In mobile IoT scenarios, the mobile IPv6 scheme can also achieve hierarchical authentication management of mobile nodes （MN, mobile node）through mobile anchors. The MN authentication information is typically stored in the home network. To optimize the frequent

interactions between MNs during access authentication and the home network authentication server, Tian Ye *et al.* [12] proposed an identity signature-based hierarchical authentication mechanism based on the implementation principle of identity-based cryptography (IBC). The hierarchical identity-based signature（HIBS, hierarchical identity-based signature） mechanism replaced the traditional public key certificate-based method and adopted hierarchical identity identification as the public key for each node. The system consisted of a root private key generator (PKG, public key generator）, several first-layer PKGs, and several second-layer users (access routers, MN, etc.). The identifier was used as a public key for each node, and the public key employed the structure of a multi-level network access identifier (NAI, network access identifier). The first layer was the PKG ID, and the second layer was the user ID. By adopting hierarchical identities, this method could be extended to designing authentication structures with more layers.

In addition, in cybersecurity research combined with blockchain technology, Zhang Bin *et al.* [13] proposed a wireless mesh network security architecture based on smart contracts. The wireless network architecture was divided into several areas (e.g., jointly built wireless networks for a park housing multiple companies or an enterprise with several departments). The purpose of this partition was to facilitate hierarchical management so a reliable routing node could be selected as the management node in each area. The management chain could have one or several management nodes on which smart contracts were deployed to manage (update or revoke) the public keys of all routing nodes in the area. All nodes jointly established a consortium contract to record the addresses of all management nodes and the smart contract addresses on them. This wireless network architecture could flexibly extend the security management of network services in specific areas.

Various countries have proposed security management strategies for their critical information infrastructure [14]. For instance, the United States has developed relatively complete, adaptive security policies and strategies for its critical information infrastructure [15]. The European Union has formulated a series of policies emphasizing the importance of coordinating member states to strengthen the cybersecurity protection of critical infrastructure [16,17]. The Cyberspace Administration Office of China also issued the *Regulations on the Security Protection of Critical Information Infrastructure* in 2017, clarifying the scope of critical information infrastructure and its protection requirements, followed by a successive array of security protection studies in China [18]. However, agreed definitions and mature research on security management of public cyberspace infrastructure are still lacking.

In summary, systematic research on security protection systems has been conducted for critical information infrastructure and other network facilities. In response to the cyberspace security issues arising in the complex and heterogeneous environment of the IoT, this study proposes strategies and suggestions from the aspects of the infrastructure itself and identity management and authentication of users.

3 Design of hierarchical authentication management based on blockchain technology

The *Criteria for Security Protection of Computer Information System* (GB 17859-1999) divides

access control into two levels: discretionary and mandatory.

Discretionary access control authorizes users based on their specified methods, whereas mandatory access control designates a unified sensitive tag for the user subject and object. The sensitive tag is classified by level, and any access must match the levels of the users and objects. Therefore, when optimizing the existing access control architecture, the advantages of blockchain technology, e.g., security, irreversibility, tamper-proofing, and transparency, can be leveraged to organize the authentication control (including identity authentication and function authentication) service system in the form of blockchain at different access control layers. For example, the top-level access control layer can be organized by various industry control nodes according to the consortium blockchain structure, which can ensure the accuracy of information through smart contracts and other means, thereby improving the authority and security of identity authentication and access control. In addition, a comprehensive design of management nodes and ordinary nodes can be performed at their corresponding levels according to practical application requirements. Specifically, one or more service nodes can be selected as the management nodes, and the nodes can be managed differently according to specific consensus mechanisms and public key generation/encryption methods. The management node can undertake the task of user registration and authentication with the upper level, as well as the management of smart contracts at the local level; whereas the other ordinary nodes only provide downward user registration and authentication management services. This decentralized service model can improve the efficiency of identity management and authentication in a hierarchical authentication architecture.

3.1 Dual authentication mechanism of management+function based on blockchain architecture

Based on the design of the authentication management architecture, the concepts of user subjects and objects in cyberspace can be extended to public infrastructure objects. This study suggests that public infrastructure should implement comprehensive access control as a basic requirement, incorporating identity attribute verification in the scope of access control messages, and further include the design of sensitive tags in the authentication mechanism of application control according to the management and allocation mechanisms of the public infrastructure. For example, in access authentication, the public infrastructure in core and public areas can be designed into top, industry, and regional levels, respectively. In access control, the technologies of blockchain and edge computing can be incorporated. Through the optimization design of sensitive tags for comprehensive hierarchical access, a 3+3 dual authentication mechanism of both management and function control can be established. In terms of access control management, it is recommended that the facilities in the core area be audited by nationally designated departments or authorized agencies, which can be called the central management nodes of national network security. The public areas should be reviewed by the industry's regulatory authorities or authorized institutions, which are referred to as the industry management nodes (e.g., power management departments). Furthermore, the management nodes can be constructed in the form of consortium blockchain. When accessing application services, the permission definition in the sensitive tag is identified, and the corresponding facilities in the area are included as regional function nodes for management, thereby improving management efficiency. The management architecture of cyberspace access control is illustrated in Fig. 2.

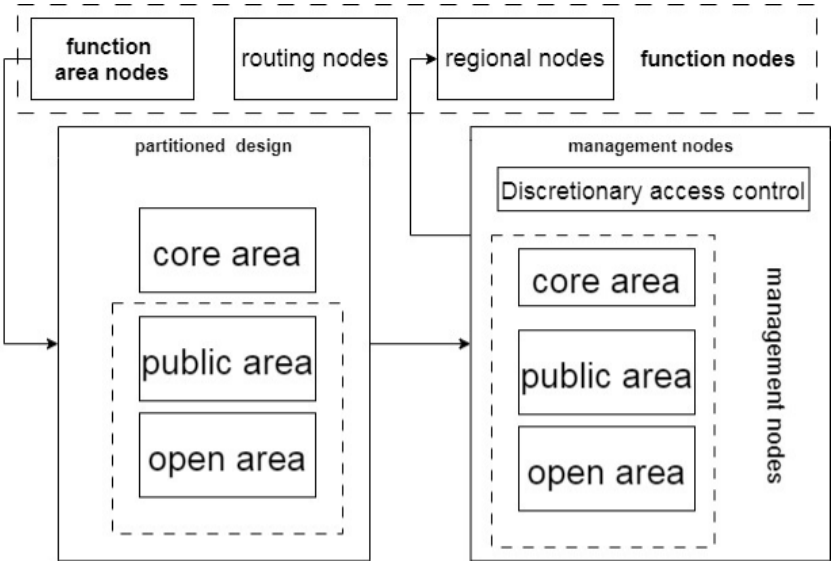

Figure 2. Network space access control management framework.

3.2 Process of dual authentication access control

Under the framework of hierarchical access control design, applications for authentication must be submitted to the corresponding management nodes when registering and maintaining certain facilities. When applying functions, the authentication requests need to be submitted to their corresponding function nodes. This hierarchical management and decentralized servicing mode can satisfy the multiple requirements in service efficiency and security. When registering public infrastructure located in public areas, applications need to be submitted to the regional and industry levels sequentially, and the interaction process is displayed in Fig. 3.

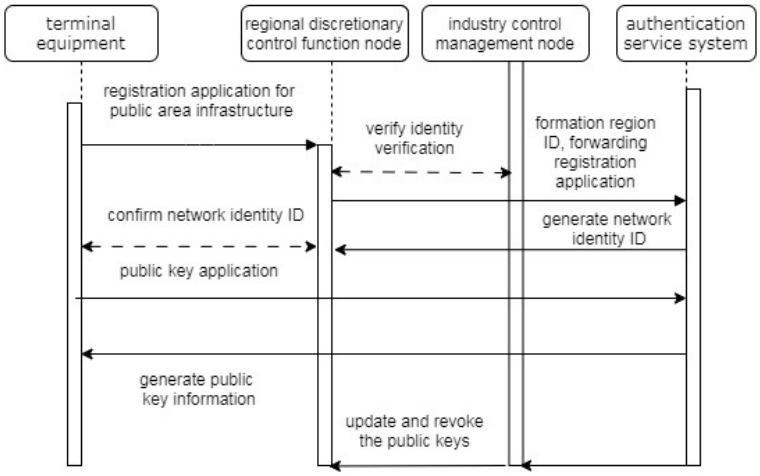

Figure 3. User interaction process.

After receiving a registration application from a terminal facility, the regional control function node requests the industry access control management node for identity verification. If the verification is passed, the unified authentication service system will generate a unique network identity ID and a sensitive tag for it. Based on the type and level of the node, matrix operation or hash function operation will be performed to generate the identity-based public key information, which will then be returned to the terminal and the corresponding function control nodes. Before requesting network connections and application services in the public infrastructure, the users need to obtain their network identity ID. The process of applying for access to a certain object is as follows. First, obtain the identity authentication and sensitive tag information of the management node on the corresponding level. Then, the management node will transfer the application to the corresponding function node for authentication. The user authentication process is shown in Fig. 4.

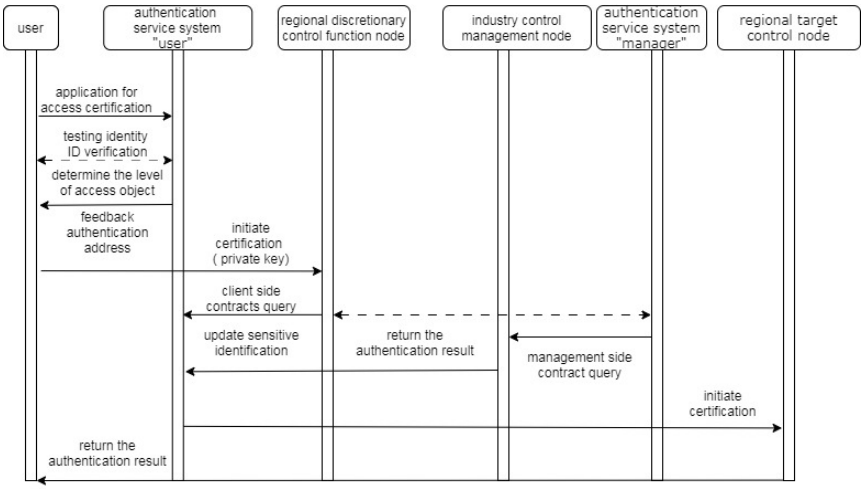

Figure 4. User authentication process.

The user first queries and verifies the regional node address through the client platform of the authentication service system and sends an authentication application to the regional function node according to the feedback. Based on the public key information, the user can perform security control operations on the regional discretionary control function node and industry control management node, such as client contract authentication and access authentication on the authentication service system side. Next, function authentication from the regional function node of the object to be accessed is performed according to the sensitive tag. If the dual authentication process is passed, access to the target device is guaranteed. Based on the aforementioned management mode, public infrastructure and its users can also be identified through a unified cyberspace identity code, including the user identity level and type in the sensitive tag. This identifier can also be used as a public key during identity authentication, thereby improving the efficiency of key management and identity authentication.

4 Conclusion

Drawing on the fundamentals of cyberspace security studies and starting with hierarchical object management and authentication methods, this paper offers suggestions on user authentication and access control management mechanisms that are suitable for the public infrastructure system in cyberspace, achieving the following improvements in network security:

(1) A centralized+distributed network service architecture is designed for network security services, which can efficiently utilize the existing basic resources in cyberspace, achieving compatibility and continuous evolution.

(2) Cyberspace security can be evaluated and configured from the perspectives of the environment, tools, and resource requirements of objects, providing more flexible object-oriented services.

(3) The management of cyberspace tools and resources with public attributes is unified, with a focus on optimizing object authentication and access control, which can facilitate a more secure cyberspace with better developments.

In conclusion, with the rapid IoT development, the traditional information security system of the Internet is facing significant security risks and challenges. To ensure cyberspace security, it is critical to study information grading and assessment management systems for trusted authentication.

References

[1] CHEN Z Z. Cyberspace: conception, characteristics and its attribution [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2019, 31(2): 63-71.

[2] KITCHIN R M. Towards geographies of cyberspace[J]. Progress in Human Geography, 1998, 22(3): 385-406.

[3] GUO L, CAO Y N, SU M J, et al. Cyberspace resources surveying and mapping: the concepts and technologies[J]. Journal of Cyber Security, 2018, 3(4): 1-14.

[4] ZHANG J, SUN Z, XU R, et al. A research on measure method of cyberspace resource[J]. Information Technology and Network Security, 2019, 38(5): 7-11.

[5] CHEN Z Z. Cyberspace: conception, characteristics and its attribution [J]. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition), 2019, 31(2): 63-71.

[6] FANG B X. Define cyberspace security[J]. Chinese Journal of Network and Information Security, 2018, 4(1): 1-5.

[7] OLIVEIRA L B, DAHAB R, LOPEZ J, et al. Identity-based encryption for sensor networks[C]//Proceedings of Fifth Annual IEEE International Conference on Pervasive Computing and Communication Workshops (PerComW'07). 2007: 290-294.

[8] ROHBANIAN M R, KHARAZMI M R, KESHAVARZ-HADDADA, et al. Watchdog- LEACH：a new method based on LEACH protocol to secure clustered wireless sensor networks[J]. Advances in Computer Science An International Journal, 2013, 2(3): 105-117.

[9] ZOU K, HOU L, JIANG Z Y, et al. Research on 3-D structure and recognition of influencing factors of information security risk in smart city[J]. Journal of Modern Information, 2019, 39(10): 15-23.

[10] ISO/IEC 29115-2013. Information technology-security techniques- entity authentication assurance framework[S]. 2013 [24] ISO/IEC TS 29003:2018. Information technology-security techniques - Identity proofing[S]. 2018

[11] ISO/IEC TS 29003:2018. Information technology-security techniques -Identity proofing[S]. 2018
[12] TIAN Y, ZHANG Y J, ZHANG H W, et al. Identity-based hierarchical access authentication in mobile IPv6 network[J]. Chinese Journal of Computers, 2007, 30(6): 905-915.
[13] ZHANG B, GUANG H, CHEN X. Smart contract-based security architecture for wireless mesh network[J]. Computer Engineering, 2019, 45(11): 16-23, 31.
[14] CAO J W, YANG M B. Energy Internet: towards smart grid 2.0[C]//Proceedings of 2013 Fourth International Conference on Networking and Distributed Computing. Piscataway: IEEE Press, 2013: 105-110
[15] XU G Q, CAO Y, REN Y Y, et al. Network security situation awareness based on semantic ontology and user-defined rules for the Internet of Things[J]. IEEE Access, 2017, 5: 21046-21056.
[16] HÄNISCH T, ROGGE S. IT-Sicherheit in der Industrie 4.0[M]. Wiesbaden, Germany: Springer, 2017.
[17] European Commission. EU cyber security strategy [R]. 2018.
[18] DONG Y N, ZHAO G X, XIE Z X. The practice of critical information infrastructure protection analysis[J]. Cyberspace Security, 2018, 9(8): 84-89.