Design and Implementation of Port Video Terminals Security Access Authentication System Using Blockchain Technology

Chunming Tang[1,a],Yuyu Ma[2*,b],Xiang Yu[3,c]

[1]Tiangong University School of Artificial Intelligence Tianjin, China
[2]Tiangong University School of Electrical and Electronic Engineering Tianjin, China
[3]Tiangong University Center for Engineering Internship and Training Tianjin, China

Abstract. In the face of the increasing scale of port video surveillance systems, edge computing is gradually used to improve the real-time processing efficiency of surveillance systems and reduce the load on the cloud with the advantages of distributed computing. In order to improve the security factor of terminal access in the edge computing environment, this paper proposes a decentralized terminal security access authentication system based on blockchain, which realizes the identity registration, revocation and mutual authentication of two interfaces between terminal devices and edge computing through the smart contract technology of blockchain, and establishes a trusted channel for data transmission between terminals and edge nodes. Through the functional test of the system and the security analysis of the system on the Hyperledger Fabric platform, it shows that the system has more security attributes and higher security.

1 Introduction

As an important channel for urban connection and foreign trade, ports play an important role in economic and social development. With the introduction of some concepts such as Industry 4.0 and Smart Manufacturing 2025, ports are also developing in the direction of intelligence. In order to improve the port's security prevention and control mechanism, a large number of terminal devices are deployed around the docks, bonded areas, automatic equipment and other areas for security monitoring. As a security method, the video surveillance system relies on the Internet of Things (IoT) and artificial intelligence (AI) technology, uses machine vision to replace human eye supervision, and uses intelligent identification to provide early warning to achieve intelligent security in the port area. The port's intelligent monitoring system is mainly divided into video monitoring intelligent platform, streaming media service module and transaction processing service. The intelligent video surveillance platform applies AI, big data and other technologies to provide data access services and control access services. The data access service is responsible for collecting, processing and distributing these real-time video streaming data from the streaming media service module in order to quickly respond to new information. By controlling access services, the platform also supports advanced functions of transaction processing services such as data persistence, result decision-making, status monitoring and data exchange. The port video surveillance system architecture diagram is shown in Figure 1.

However, as the scale of video surveillance continues to expand, the access of a large number of terminal devices will inevitably bring security risks. Such as video data leakage, virus transmission and Trojan horse implantation caused by video front-end access and counterfeit access. Terminal authentication is the first step for a device to access the network and the first barrier to network security. Two-way authentication needs to be established between the terminal and the IoT application to ensure the two-way identity security of the system and the source of IoT collection data.

Blockchain technology, which arose along with the digital currency Bitcoin [1], is a distributed data ledger with features such as network-wide consistent consensus, decentralization, programmability and security against tampering, and has natural advantages in transmitting trust. Using blockchain to address IoT terminal identity authentication has the following advantages: (1) Blockchain has decentralized characteristics, even if one node fails, other nodes will not be affected and will not affect the work of the whole system, thus avoiding the problem of single point of failure of traditional CA nodes. (2) After the data is released and uploaded to the blockchain by consensus, it is jointly maintained by each node to ensure the validity of the data and not to be tampered with. (3) The distributed nature of the blockchain can meet the network access requirements of IoT devices in sports scenarios.

[a]tangchunminga@hotmail.com [b]mayuyuxxxx@163.com [c]1922489185@qq.com

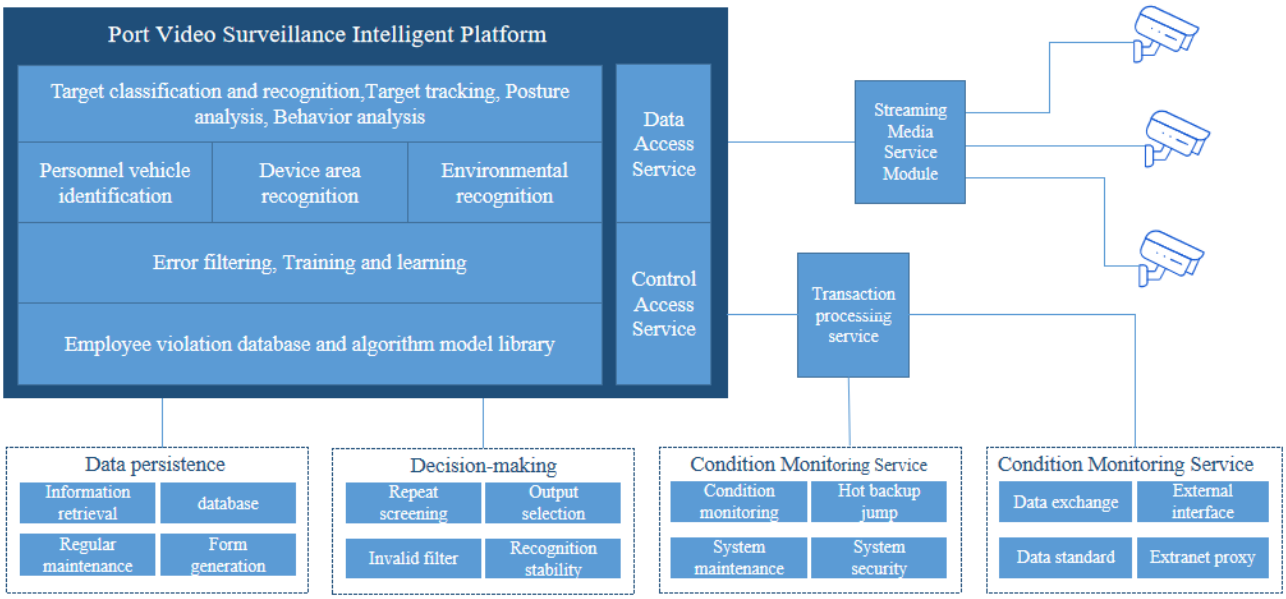

Figure 1. Port video surveillance system architecture.

Therefore, this article introduces blockchain technology to propose a decentralized, distributed and open and transparent terminal identity authentication system.

The other sections of this paper are organized as follows: Section II introduces the related work of identity authentication. Section III proposes a secure access authentication scheme for IoT terminals. Experimental verification and security performance analysis are given in Section IV. Finally, the conclusion is given in Section V.

2 Related Work

IoT terminal identity authentication is a hot spot in the research of Internet of Things security technology. Traditional identity authentication schemes include the following three types: authentication based on symmetric keys [2], authentication based on public key infrastructure (PKI) [3], and identity-based cryptograph (IBC) [4]. The authentication scheme based on the symmetric key occupies less system resources, has a fast encryption speed, and does not require the access of a third-party trusted organization. It is a completely decentralized authentication method. In this type of scheme, when the symmetric key is shared for the first time, it is necessary to ensure that the information channel through which the symmetric key is transmitted for the first time is absolutely secure, otherwise the scheme cannot guarantee the security of the symmetric key sharing process. PKI-based certification requires the establishment of a strong authoritative certification authority as a centralized third-party trusted authority. In large-scale IoT device application scenarios, this type of certification authority needs to invest a lot of manpower and material resources to issue and manage digital certificates. The IBC authentication is proposed on the basis of PKI. Although this scheme has a solution to the certificate management and transmission problems in the PKI-based authentication scheme, it requires a trusted third party to generate a private key for the device. In addition, complex calculations such as bilinear pairing are required, and the computational overhead is relatively large.

As blockchain has the characteristics of decentralization, data tamper-proof and traceability, it can be well combined with IoT application scenarios. In recent years, a number of scholars have tried to apply blockchain technology to the field of identity authentication. The literature [5] uses blockchain technology to improve PKI technology and achieve distributed PKI authentication, which solves the problems of traditional PKI such as single point of failure and certificate transparency. Literature [6] combines blockchain with edge computing, and uses edge computing to support edge authentication services in blockchain systems. Established a distributed and credible authentication mechanism, realized two-way authentication, and improved authentication efficiency. Literature [7] based on fuzzy extraction theory and combined with blockchain technology, proposed a two-factor authentication mechanism scheme for biometrics and passwords, which uses a collision-resistant key negotiation mechanism between biometric collectors and blockchain nodes to ensure security during communication and achieve cross-domain authentication of identity.

3 Design of Terminal Security Access Authentication System

Edge computing [8] is a new computing model that performs computing tasks at the edge of the network. It can optimize delays by offloading computing tasks. Compared with cloud computing [9] models, it can respond to user needs more quickly, reliably and energy-savingly. The port video surveillance system will take up more bandwidth resources when the camera transmits video data to the central server, which will put tremendous pressure on network transmission. In this case, the port video surveillance system uses edge computing technology to reduce the network load of the central server while improving the efficiency of video image analysis

and processing. This system is designed to solve the security access authentication problem of port video terminal equipment in the edge computing environment.

3.1 System Model

This system uses a consortium blockchain [10], which is one of the blockchain types. The consortium blockchain in the blockchain has the characteristics that users cannot access without authorization, ensuring the privacy of data information. The system model structure is shown in Figure 2, which mainly includes the blockchain and the blockchain port for external calls. Terminal devices and edge nodes can implement identity authentication, query, and revocation by calling the interface. The specific process is as follows: When an IoT device leaves the factory, a public key, private key and digital signature are generated, written by the manufacturer to the device, and submitted to the blockchain identity system for publication. After the blockchain identity authentication system is verified, the identity data is recorded in the blockchain. Edge computing nodes also register their identity data in the blockchain. When a connection needs to be established between the IoT terminal and the edge computing node, the IoT terminal sends the identity mark to the edge computing node, the edge computing node queries the identity data to the blockchain identity authentication system according to the identity mark, and the identity authentication system returns the identity data and the authentication status. The edge computing node authenticates the device based on the queried information, and the IoT device authenticates the edge computing node in the same way. After that, both continue the Transport Layer Security (TLS) handshake process to establish a secure data transmission channel.

3.2 Smart Contract and Key Process Design

The key to the model designed in this article is the smart contract [11] module. The smart contract is divided into two parts: the user's identity data and the interface functions that can be called externally. The following section describes how to implement the registration, query and revocation processes in the model through smart contracts.

(a) Registration process

The registration process is mainly a process in which the terminal device and the edge node call the RegisterIdentity function (as shown in Algorithm 1) in the smart contract after verification by the verification node, and write their identity data into the blockchain.

Terminal device is used as an example: Terminal device to verify node sends identity plaintext data Info as well as the private key sk on the Info after the hash operation signature value sign (sk, InfoHash), the verification node first checks whether the format of the terminal device Info is wrong, and if it is wrong, it returns a failure response. If there is no error, store Info and the designated verification node signer, set the public key address ownerAddr to the public key address of the caller (msg.sender), and generate the unique identification ID of the identity data. Then the verification node checks the authenticity of the data, and the specific method is as follows. The verification node decrypts the digital signature with the sender's public key to obtain the digest value InfoHash of the identity data, and then calculates whether the Hash (Info) and InfoHash are equal. If they are equal, it means that the identity of the terminal device is legal and the data has passed the verification. The verification node sets the authentication status to pass and sets the expiration time to expireDate. After the user's various identity information is submitted to the blockchain by the verification node, the majority of the nodes in the consortium blockchain reach a consensus and record it in the blockchain. Finally, the event of exitConfirmEvent is triggered and the success response is returned. After receiving the success response, the terminal device stores the identity data uniquely identifies the ID, the authentication node and the identity expiry time for use in subsequent authentication.

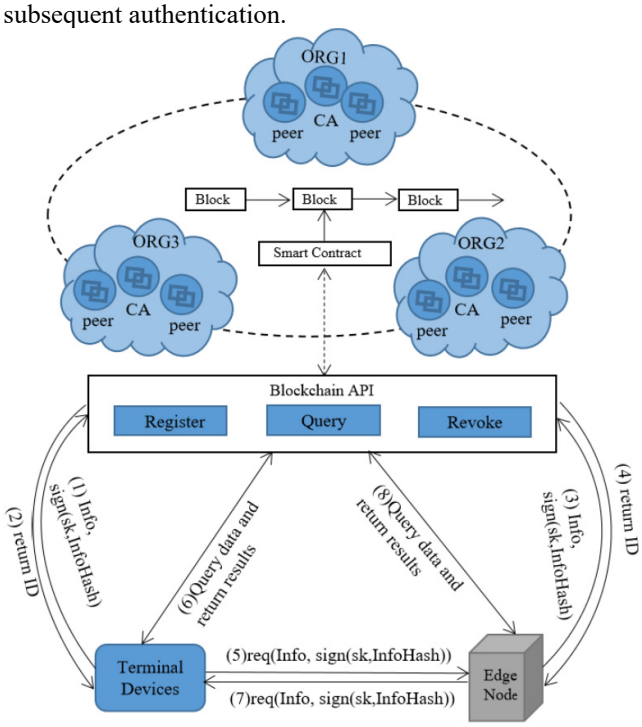

Figure 2. Blockchain-based secure access model of terminal device.

Algorithm 1: Register identity data
Input: ID, Info, ownerAddr, signer
Output: success/error
function RegisterIdentity(ID, Info, ownerAddr, signer)
userIdentity = UserIdentity[ID]
userIdentity.Info = Info
userIdentity.ownerAddr = msg.sender
userIdentity.signer = signer
if msg.sender = userIdentity.signder then
userIdentity.status = pass
userIdentity.expiryDate = expiryDate
emitConfirmEvent(ID, msg.sender, expiryDate)
return success
else
return error
end if
end function

(b) Query process

The query process mainly refers to the process in which the edge node queries and verifies the authenticity of the terminal device's identity data through the blockchain when the terminal device establishes a connection with the edge node. Similarly, terminal device also needs to verify the security of the edge node's identity.

The specific process is as follows: First, the terminal device sends a data upload request req(ID, Info, sign(sk, InfoHash)) to the edge node, and the edge node obtains the corresponding Info, ownerAddr, signer and other identity data through the smart contract according to the ID for identity verification. The specific steps are as follows. (1) Verify that the Info provided by the device is consistent with what has been stored to ensure the authenticity of the data provided by the user. (2) Verify the signature value sign (sk, InfoHash) of the device to ensure that the device has the corresponding private key and ensure the device's ownership of the identity data. (3) Check whether the signer is the address of the trusted node, and ensure that the piece of data is verified by the trusted node. (4) Check whether the authentication status is pass and whether the current time exceeds the expiryDate. If all the above conditions are met, a response message of successful authentication is returned, and the terminal device verifies the edge node in the same way.

(c) Revoke process

The revocation process mainly refers to the process of the authentication node modifying the authentication status of the specified published identity data. The authentication status is modified from pass to revoke by calling the RevokeIdentity function in the smart contract (as shown in Algorithm 2): (1)Check whether the caller is a signer, if it is not, the revoke operation cannot be performed; (2)Modify the authentication status corresponding to the specified identity data identifier ID to revoke; (3)Trigger the revoke event emitRevokeEvent, so that the application can update the latest data in time, and can be detected in time without the CA authority releasing the revocation certificate list regularly.

```
Algorithm 2: Revoking identity data
Input: ID
Output: success/error
function RevokeIdentity(ID)
userIdentity = UserIdentity[ID]
if   msg.sender = userIdentity.signder   then
userIdentity.status = revoke
emitRevokeEvent(ID, msg.sender)
    return success
else
    return error
end if
end function
```

4 Experimental Results and Evaluation

4.1 Simulation analysis

In order to verify the feasibility of the proposed method, we conducted a simulation analysis. The working environment is as follows: Intel(R)Core(TM)i5-10400 CPU @2.90GHz processor, 32GB RAM, operating system Ubuntu18.04 (64-bit). The experimental platform is Hyperledger Fabric version 2.2, and the feasibility of smart contracts is tested on the test network. Figures 3 to 5 show how users call functions in the smart contract. Figure 3 shows the RegisterIdentity function called during user identity registration. Figure 4 shows the user querying the identity data of the specified ID through the QueryIdentity function. Figure 5 shows the verification node modifying the identity authentication status of the specified ID from pass to revoke through the Revoke Identity function. The results show that the user's identity registration, query, and revocation can be completed through the smart contract.

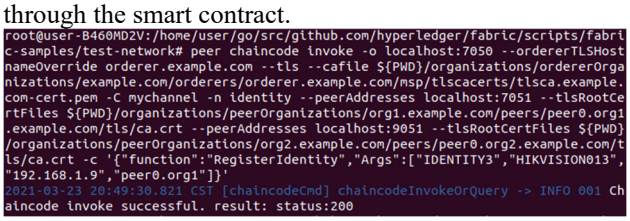

Figure 3. Identity registration.

Figure 4. Query identity.

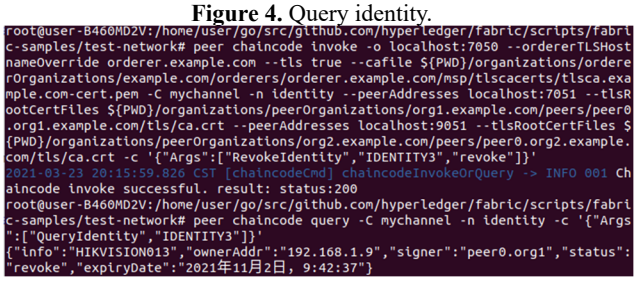

Figure 5. Revocation of identity authentication status.

4.2 Safety Analysis

We compare the terminal authentication scheme (TA) proposed in this article with some distributed identity authentication schemes, such as KPSD [12], EAAP [13] and EPAW [14] in terms of security attributes. As shown in the table, we mainly analyze 5 key security attributes: two-way authentication, privacy protection, traceability, anti-forgery attacks and anti-forgery attacks. √ in the table indicates that the considered scheme meets the specific security attribute, and × indicates that the considered scheme does not meet the specific security attribute.

TableI. Comparison of security attributes

comparison item	KPSD	EAAP	EPAW	TA
two-way authentication	×	√	√	√
privacy protection	√	√	√	√
traceability	×	√	×	√
anti-forgery attacks	√	√	√	√
anti-forgery attacks	×	×	×	√

We will analyze the security attributes of this solution TA below. First, during the registration process, the verification node needs to verify the identity submitted by the user to confirm the authenticity of the user's identity data. After the verification is passed, the verification node submits the identity data to the consortium blockchain, and most nodes reach a consensus before it can be written into the blockchain. If the verification node has issued false data, the identity issued by the node will no longer be trusted after verification and discovery, thus resisting Abuse of power. After the user's identity information is verified and recorded on the blockchain, no entity other than the members of the consortium blockchain can obtain the identity data in the ledger, ensuring the privacy of the identity data. Every transaction on the blockchain is transparent and traceable, which can prevent nodes from deliberately leaking the true identity of the device. With the blockchain as the cornerstone of trust, terminal devices and edge nodes can achieve two-way authentication of identities through the blockchain identity authentication system. If a malicious node wants to forge the identity of the device to send information to the node, it needs to obtain the user's unique identification ID, the user's detailed identity plaintext data Info, and the user's private key sk. Because the private key is highly confidential and does not participate in the transmission, it is difficult for malicious nodes to forge the identity of the device, which proves that this scheme can resist forgery attacks. In summary, this solution satisfies all the security attributes compared. KPSD scheme does not consider two-way authentication; KPSD and EPAW schemes do not meet traceability; and the KPSD, EAAP and EPAW do not consider the constraints of authority power and do not satisfy resistance to power abuse. From the comparison results, it can be seen that the scheme in this paper satisfies more security attributes and is more secure compared with other schemes.

5 Conclusion

Combining the environmental characteristics of edge computing and the IoT, this paper proposes a blockchain-based IoT terminal security access authentication scheme. This scheme is suitable for port video surveillance systems, which solves the shortcomings of traditional identity authentication systems and improves the security of data access at edge nodes. At present, the prototype system is only for experimental verification in a stand-alone environment, without cluster deployment in the sense of production. Future work will continue to improve the prototype system, develop a fully functional front-end page, and conduct research and improvement on the consensus algorithm.

References

1. D. Yermack, "Is bitcoin a real currency? ", SSRN Electronic Journal, pp.31-43, 2013.
2. J. H. Han & J. N. Kim, "A lightweight authentication mechanism between IoT devices", International Conference on Information & Communication Technology Convergence, pp.1153-1155, 2017.
3. S. Sciancalepore, G. Piro, G. Boggia & G. Bianchi, "Public key authentication and key agreement in iot devices with minimal airtime consumption", IEEE Embedded Systems Letters, 9(1), pp.1-4. 2017.
4. W. LiZhen, Z. Longjun, "Hybrid mutual anonymous authentication protocol for the Internet of things environment", Application Research of Computers, pp :222-225, 2015. (In Chinese)
5. T. Feng, W. Chen, D. Zhang & C. Liu, "One-Stop Efficient PKI Authentication Service Model Based on Blockchain". CCF China Blockchain Conference. Springer, Singapore, 2019.
6. S. Guo, X. Hu, S. Guo, X. Qiu and F. Qi, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System", IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp: 1972-1983, March 2020.
7. Z. Haodi, L. Guorong, W. Laifu, et al. "Research on cross-domain identity authentication mechanism based on blockchain technology", Guangdong Communication Technology, pp. 23-31, 2018.
8. M. Satyanarayanan, "The Emergence of Edge Computing," in Computer, vol. 50, no. 1, pp. 30-39, Jan. 2017.
9. Vouk M A . Cloud Computing[C]// International Conference on Information Technology Interfaces. IEEE, 2008.
10. N. Lu, Y. Zhang, W. Shi, S. Kumari & K. Choo, "A secure and scalable data integrity auditing scheme based on hyperledger fabric". Computers & Security, pp. 101741.1-101741.16. May, 2020.
11. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292-2303, 2016.
12. J. Shao, X. Lin, R. Lu and C. Zuo, "A Threshold Anonymous Authentication Protocol for VANETs", IEEE Transactions on Vehicular Technology, vol. 65, no. 3, pp: 1711-1720, March 2016.
13. M. Azees, P. Vijayakumar and L. J. Deboarh, "EAAP: Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 9, pp: 2467-2476, 2017.
14. S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam and J. D. Almakhles, "EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs)," IEEE Access, vol. 8, pp: 48576-48586, 2020.