Security Threat Early Warning of Distance Education System Based on Blockchain

Zhihua Chen[1], Gautam Srivastava[2,3,4]*

[1] Network Information Center, Guangdong Polytechnic Normal University, China
[2] Research Centre for Interneural Computing, China Medical University, Taiwan
[3] Department of Math and Computer Science, Brandon University, Canada
[4] Department of Computer Science and Math, Lebanese American University, Lebanon
czh@gpnu.edu.cn, srivastavag@BrandonU.ca

Abstract

To ensure the safe and stable operation of distance education systems, a security threat early warning technology based on blockchain is proposed for distance education system, which builds a security threat warning model. It uses the data interface in the interface layer to connect the teacher and student client. Then, the network behavior data of the distance education system is collected and transmitted to the data layer, where data blocks exchange the behavior data of the distance education system, and then the chain structured behavior data is generated and transmitted to the consensus layer. After the behavior data is transmitted to the incentive layer through the consensus layer, the distribution mechanism and basis are used to process and transfer the behavior data to the contract layer. The contract layer uses the threat early warning model to calculate the behavior data, and then conducts threat rating and early warning response on the data. It transmits the threat rating and early warning results to the application layer and presents them to users, thus realizing the security threat early warning of the distance education system. The experimental results show that the transcoding rate of this technology for the network behavior data of the distance education system is higher than 0.97, the early warning accuracy for the 10 types of network data of the distance education system can reach 100%, and the credibility of the early warning security threat of the types of DDOS IP, DDOS IP, phishing website URL address, and mobile malicious server IP address is higher than 0.96. Therefore, the technology has a strong capacity of behavior data storage in distance education systems, and can effectively warn different types of security threat in distance education systems. It has a more excellent application effect.

Keywords: Blockchain, Distance education system, Security threat information, Early warning technology, Information early warning

1 Introduction

The hidden dangers of network security, such as virus attack, hacker attack, Sybil attack [1], data tampering and leakage occur frequently in the distance education system, threaten the information and network security of education departments and schools at all levels [2]. Under the background of increasingly complex network security attacks, network security situation assessment [3] has become the premise to ensure network security.

However, it cannot effectively prevent attackers from obtaining local attack information by only relying on the technical strength of individuals or individual organizations. The sharing of security threat information [4] of distance education system can make timely use of the effective threat information generated in other networks to improve the response ability of the defense party, shorten the response time, and achieve the effect of "single point perception and network wide defense". Modern technologies such as multi-source information cleaning and merging technology, Internet asset portrait technology, big data association analysis technology, and machine learning technology [5] have been used, which are combined with threat early warning, equipment linkage intelligent defense, hot event emergency handling, tracking and tracing, attacker portrait, positioning counter measures, and other means to build a three-dimensional collaborative defense ecological platform through cloud land integration.

The platform can reduce the cost of information collection, optimize the problem of information islands, and improve the threat detection and emergency response capabilities of all parties involved in sharing. It promotes effective prevention, control and resistance of information security risks [6], and improves the overall security protection level. For this reason, there are also many scholars studying security threat information early warning technology.

Ammi, M, et al. [7] proposed a cloud native architecture network threat information early warning method, which obtains the current network security threat information IP by building a network cloud native architecture. It uses early warning technology to realize the security threat information early warning of distance education system. Riesco, R et al. [8] embed a security threat information detection method of distance education systems into the blockchain based on blockchain technology. When security threat information is detected in the current network, an early warning is sent to the user by generating blockchains. Waqas, M. et al. [9]

*Corresponding Author: Zhihua Chen; E-mail: czh@gpnu.edu.cn
DOI: 10.53106/160792642023092405013

put forward an artificial information network security early warning method. This method combined artificial information and machine learning algorithms to review the security types and threat types in the network, and then sent users a distance education system security threat type early warning.

In combination with the characteristics of blockchain technology [10-11], such as distribution, transparency, traceability and openness, this paper proposes a security threat information early warning technology for distance education systems based on blockchain. Based on the analysis of the security threat information early warning blockchain structure of the distance education system, the security threat information early warning design of the distance education system is realized from two aspects: the safe exchange of the behavior data of the distance education and the optimization of the threat information early warning process. Through the application of this technology, the information threatening the distance education system can be warned in time to ensure the safe and stable operation of the distance education system.

2 Application Analysis of Blockchain in Distance Education System

2.1 Consensus of Distance Education Activities

The consensus mechanism is the basis and core of blockchain technology [12], which determines the way in which participating nodes reach agreement on certain specific data. In the blockchain system using the point-to-point network mechanism, the sequence of distance education events corresponding to each node is different due to the existence of problems such as sequence and network delay. Therefore, it is necessary to design an effective mechanism to reach a consensus on the sequence of events within a certain period of time. The distance education resource providers and users also need to be encouraged to implement disciplinary mechanisms against nodes that disrupt the operation of distance education blockchain. This kind of mechanism depends on some ways to determine the role of new block generation sequence [13].

2.2 The Immutability of Distance Education Records

The system storage, transmission structure, and operation mode based on the blockchain [14] can effectively constrain the participants, and provide mutual trust between teachers and students in the use records of distance education. When the learning of distance education is completed by students, a new block will be created to record the learning information, which will be sent to all nodes in the network for verification. After the verification is completed, the blockchain will broadcast to each node. Since the modification of the block involves the modification of the hash value, and the calculation of the hash value is time-consuming, it is difficult to modify multiple blocks at the same time.

2.3 Traceability of Distance Education Process

Block chain technology can provide a time stamped record of the learning process, which can realize the whole cycle of learning process supervision, so as to effectively eliminate problems such as plagiarism in homework and distortion in course viewing records. Block chain allows all nodes in the whole network to stamp a timestamp on each block for bookkeeping to indicate that this information is written at this time. In this way, a database that is not tampered with and forged is formed. A time stamp can prove that someone did something on a certain day and who the first creator of an activity was. The proof of "existence" of anything becomes very simple. Every transaction data on the blockchain [15] can be traced back through the chain structure, and every learning data can be verified. Therefore, every transaction made on the block chain is traceable.

2.4 Decentralization of Learning Resources

The direct interaction of the point-to-point network of the block chain avoids the monopoly of the central node on learning resources, and also saves the cost of learning resource transmission. The server can be set up by different institutions or organizations as a node on the blockchain, and each node is in a parallel relationship [16]. When one node updates data, the other nodes will be consistent, and all data will be updated by consensus. The characteristic of distributed accounting of smart contracts in blockchain technology [17] builds customized links between learners and learning resources, according to the specific characteristics of learners. In the process of pushing and managing resources on the network, distributed features are used for decentralized and networked storage. It realizes the point-to-point link between learners and resources based on block chains, and also achieves resource sharing, thus reducing unnecessary access and resource waste [18].

3 Structure of Security Threat Early Warning Blockchain in Distance Education System

According to the analysis in Part 2, the application prospect of blockchain technology in distance education systems is relatively broad. Therefore, when studying the security threat information early-warning technology of distance education systems based on blockchain, this paper analyzes the security threat information early-warning blockchain structure of distance education systems on the technology of application analysis of blockchain technology in distance education systems.

The security threat information early warning model of distance education systems is built on the basis of blockchain technology, and the structure of the model is shown in Figure 1.

The security threat information early warning model of distance education system based on blockchain consists of interface layer, data layer, consensus layer, incentive layer, contract layer, and application layer.

The interface layer is connected by students and teachers, respectively, through which the behavior data of teachers and students on the distance education system is transmitted to the data layer.

The data layer uses data blocks to store the behavior

data of the distance education system, and then generates the behavior data chain structure, and then transmits it to the consensus layer.

The consensus layer combines the consensus methods of POW, POS, and DPOS to share and process the behavior data of teachers and students with chain structure. The distribution mechanism within the incentive layer distributes the data chain structure of teachers' and students' behavior.

After the threat sharing model in the contract layer shares the behavior data of teachers and students in a chain structure, it will be used as the input to start the threat information early warning response algorithm, output the threat information early warning response results existing in the current behavior data of teachers and students, use the results as the input, and use the threat information rating method to obtain the threat information level in the behavior data of teachers and students. The application layer outputs and displays the security threat information early warning response results and rating results to users.

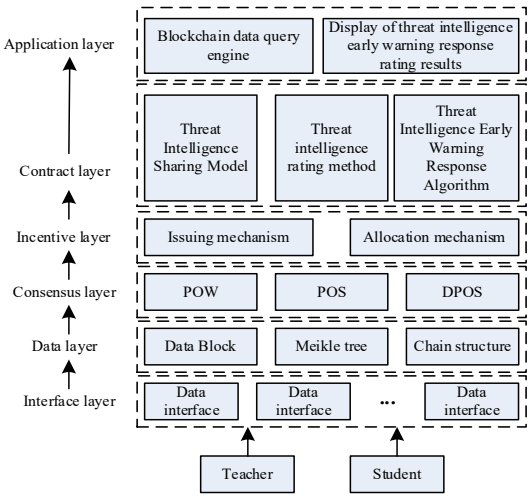

Figure 1. Security threat information early warning model of distance education system based on block chain

Considering that the security threat information early warning technology of the distance education system based on the blockchain mainly acts on the data layer in Figure 1, which is the general ledger of data shared by distributed nodes in the decentralized system. Each node can package the transaction orders received within a certain time into a time stamped data block through a specific hash algorithm and Merkle tree [19] data structure. Then, it can link the data block to the current longest main chain to form the latest blockchain.

Each data block consists of two parts: the block header and the block body. The block header encapsulates the current version number, the previous block hash value, the current block hash value, the random number of the current block Proofofwork (PoW) consensus process, the Merkle root, and the timestamp. The block body includes the total number of transactions in the block and all verified transaction records. After the hash process of Merkle tree is calculated, the unique Merkle root is finally obtained. Only the Merkle root finally calculated needs to be recorded in the block header.

4 Design of Security Threat Early Warning for Distance Education System

According to the analysis of the security threat information early warning blockchain structure of the distance education system, when a security threat occurs to the distance education system, it mainly acts on the data layer of the blockchain structure. Therefore, the design of security threat information early warning of distance education system is carried out from two aspects: safe exchange of behavior data of distance education and optimization of threat information early warning process.

4.1 Safe Exchange of Distance Education Behavior

In the data block of the data layer, it uses the distance education behavior data encryption control method to securely exchange the distance behavior data between students and teachers. The purpose of distance behavior data encryption control is to control access rights during data security exchange, avoid malicious calls by illegal persons during data exchange of distance education behavior, and improve the security exchange level of distance education behavior data. The RSA encryption algorithm [20] is used to call block chain technology to complete the security exchange of data. Therefore, the encryption control of distance education behavior data is completed by controlling the access control permission of block chain technology. In this paper, RSA symmetric encryption algorithm is used to design the data encryption control method of distance education behavior, which ensures the safe exchange of data by controlling the aggressiveness of distance teachers' and students' behavior to access data. The algorithm formula is shown in Formula (1):

$$com = (pk_{ziE}^{u,s}, pk_{sig}^{s,u})(com_{u,s}^{public}), \quad (1)$$

where com is the encryption symmetric formula; $pk_{ziE}^{u,s}$ represents the identity of the data; $pk_{ziE}^{u,s}$ denotes the public key of the data; $com_{u,s}^{public}$ reports the public key of the distance education system device.

The data to be stored is modified by RSA symmetric encryption algorithm through block chain technology. Meanwhile, the data processed by the algorithm is hexadecimal bytes and has irreversibility, which increases the difficulty of data cracking. In the process of data security exchange, the hash algorithm is used to transcode the binary byte data without changing the content of the data. Because the distance education behavior data is mobile in the process of security exchange, the private key is used for data transcoding in this paper.

Through the above analysis, the data security exchange process of data block chain based on block chain technology is designed, as shown in Figure 2.

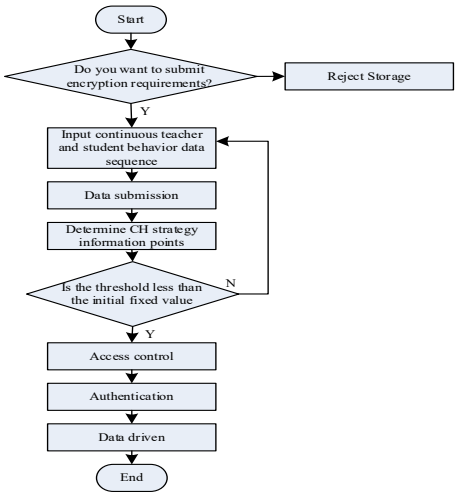

Figure 2. Storage process of distance data encryption storage method based on block chain technology

Step 1: First judge whether the remote education behavior data to be exchanged has submitted encryption requirements. If yes, go to Step 2; If not, reject the exchange.

Step 2: After inputting and submitting a continuous sequence of network behavior data, determine the CH strategy information point (script interpreter in the blockchain).

Step 3: Calculate the network behavior data access threshold according to the policy information point determined in Step 2, and judge whether the threshold is less than its initial fixed threshold. If yes, go to Step 4; If not, continue to input continuous network behavior data sequence.

Step 4: After the controller accesses and authenticates, drive the data.

After repeated iteration of the above steps, the network behavior data security exchange of the distance education system is realized.

4.2 Optimize the Threat Information Early Warning Process

Threat information early warning model is used to realize threat information early warning of distance education systems. A block chain has the characteristics or functions of decentralization, account anonymity, openness, autonomy, immutability, and smart contract mechanism. It can meet the requirements of privacy protection, reward based on contribution value, traceability of threat information, automatic early warning response, etc. in the security threat information early warning of distance education system, including:

(1) The anonymity of the block chain protects users' privacy, to a certain extent. But it also provides convenient conditions for malicious attack users to hide their identities.

(2) The traceability of the block chain is determined by the construction process of the blockchain, *Block* (*N*) = *Hash* (*tp*(*N*), *Merkle* (*N*), *Block* (*N* − 1), *nounce*), where *Block* (*N*) represents the block chain structure; *tp*(*N*) is the time stamp; *Merkle* (*N*) = *Hash* (*Tx*(*N*)) reports the root of *Merkle* containing existing transactions; *nounce* denotes a random number.

(3) The smart contract can trigger transactions when it meets the contract conditions of Formula (2):

$$is \quad execute = \begin{cases} True, x \in conditions \quad or \quad x = conditions; \\ False, otherwize \end{cases} \tag{2}$$

In formula (2), *Conditions* represents a smart contract.

In view of this, this paper optimizes the security threat information early warning process of the distance education system according to the specific block chain structure, as shown in Figure 3:

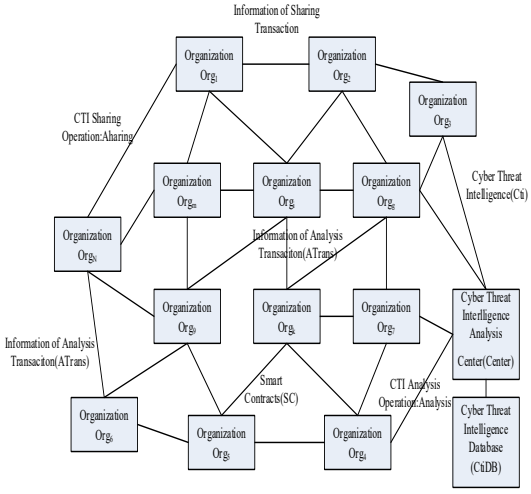

Figure 3. Block chain based security threat information early warning model structure

As shown in Figure 3, the security threat information early warning process of distance education system is represented by octets <*Org*, *Center*, *BlockNet*, *CtiDB*, *Cti*, *Trans*, *SC*, *Operation*>, where *Org* refers to the organization, which can give early warning of the security threat information of the distance education system; There are *N* organizations $Org_i (1 \le i \le N)$ in the model. Each organization Org_i serves as a node of the blockchain and has the address O_{acc} of the blockchain account; The organization appears in the form of O_{acc} in the process of security threat information early warning of distance education system, which can effectively protect the identity information of organizations. *Center* refers to the security threat information analysis center of distance education system, which has an early warning function and is an indispensable trusted third party for inference construction of a complete attack chain. It has a block chain account address. *BlockNet* represents the block chain network, which is composed of *Org* and *Center*; *CtiDB* indicates the security threat information database of the distance education system, which can store the security threat information of the distance education system. The information in the security threat information database of the distance education system is encrypted information *Hash*(*Cti*), which can effectively prevent the disclosure of private information in the information. *Cti* represents the security threat information of the distance education system

Cti ∈ {*OneCti*, *TwoCti*}.

This paper mainly discusses the monistic and dualistic security threat information, and the other multi category security threat information can be divided into the combination of multiple dualistic or monistic security threat information of distance education system. *Trans* refers to the transaction information on the block chain, which includes the security threat information early warning transaction of the distance education system, i.e. *Trans* ∈ {*STrans*, *ATrans*}. *SC* refers to the smart contract created by the organization, which is composed of the creator's account address O_{acc}, trigger conditions, early warning *response*, and information use costs *uf*. When *Center* finds that the triggering conditions *condition* of the smart contract are met in the information analysis and reasoning, it will execute the early warning *response* and deduct the expenses *uf* from the creator's account address O_{acc} of the smart contract. *Operation* denotes the action operation among subjects *Org*, *Center*, *CtiDB* and *BlockNet*. It includes information node registration (*registry*), security threat information early warning (*sharing*), information evaluation (*evaluate*), threat information analysis (*analysis*), transaction broadcasting (*broadcast*), information storage (*store*), information extraction (*get*), and smart contract creation (*create*). When organization Org_1 and *Center* conduct information early warning, various actions such as *sharing*, *get*, *evaluate store*, *broadcast* will be involved by different subjects. The early warning process of the information early warning model is as follows:

Step 1: The threat information provider generates information information and outputs it to Step 2.

Step 2: The upload interface is used to upload threat information information, and the threat information information enters the security threat information block chain early warning in Figure 3, that is, the output of step 1 is received and uploaded.

Step 3: The output of Step 2 is received, which is used to record threat information. For the repeated information information, an algorithm based on the fusion of time series and quality series is set, which greatly reduces the repetition rate of information information.

Step 4: Generate blocks: the output of Step 3 is received and blocks are generated.

Step 5: Broadcast block: the output of Step 4 is received for broadcast of the block.

Step 6: The block is written into the blockchain to alert the security threat of the distance education system.

4.3 Implementation of Security Threat Information Early Warning of Distance Education System

According to the above steps, the security threat information early warning of distance education systems is realized. However, due to the rapid progress of some attacks and threats, there remains a need to improve the early warning speed in the blockchain network for security threat information of the distance education system. Based on the above research, this paper introduces the early warning response mechanism based on smart contract to further optimize the security threat information early warning performance of distance education systems. The detailed algorithm flow is shown in Table 1:

Table 1. Early warning response algorithm

Input: account address of the creator of the smart contract O_{acc}, conditions of the smart contract *condition*, alerts *response*, and paid fees *uf*.
Output: threat information that meets the conditions of smart contract *Cti*.

1) *sera*(*msg,CtiDB*)
2) *The organization is used for execution:*
3) *Sc=create_sc*(*condition,response,uf*);
4) *Broad_to_blockchain*(*sc*);/*Broadcast smart contract in the information blockchain network*/
5) *CTI Center is used to perform:*
6) *If Cti match condition*
7) *Execute*(*response*);
8) *arrans=construct_atrans*(*Cti*);
9) *broad_to_blockchain*(*atrans*);
10) *return SEnc*(O_{pub_k},*Cti*);
11)*end if*

Combined with the early warning response algorithm based on smart contract shown in Table 1. The current threat information level of the distance education system is output through the contract layer in the security threat information early warning block chain structure of the distance education system to achieve security threat information early warning of the distance education system. The process is shown in Figure 4:

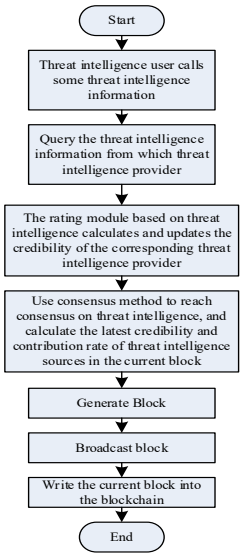

Figure 4. Blockchain based threat information rating method flow diagram

The block chain based threat information rating method includes the following steps:

Step 1: The threat information user invokes a threat information message.

Step 2: Query the source of threat information. That is, receive and query the output of Step 1.

Step 3: The rating module based on threat information is calculated and the credibility of the corresponding threat information provider is updated. That is, the output of Step

2 is received, and the credibility of the threat information source is calculated and updated.

Step 4: The latest credibility and contribution rate of the threat information source are recorded in the block. That is, the output of Step 3 is received to record the latest credibility and contribution rate of the threat information source.

Step 5: Generate blocks: the output of Step 4 is received for block generation.

Step 6: Broadcast block: The output of Step 5 is received for block broadcasting, and then the current block is written into the block chain to end the rating. The rating rules of threat information are as follows: when the credibility is within the range of 0.2-0.5, it belongs to the first level early warning. At this time, the security threat of distance education system is low and can be ignored; When the credibility is in the range of 0.5-1.0, it belongs to the second level early warning. At this time, the security threat of the distance education system is relatively high, and relevant personnel need to be reminded; When the credibility is greater than 1.0, it belongs to the third level early warning. At this time, the security threat of the distance education system is very high, so it is necessary to send out the early warning signal in time and deal with it.

5 Experimental Analysis

5.1 Experimental Setup

The object of the experiment is a distance education system. The distance education system has open classes, small classes and independent live studios, which can meet the needs of teachers' personalized live scenes with low delay. It can realize two-way video and intimate interaction between teachers and students. The network topology of the distance education system application environment is shown in Figure 5.

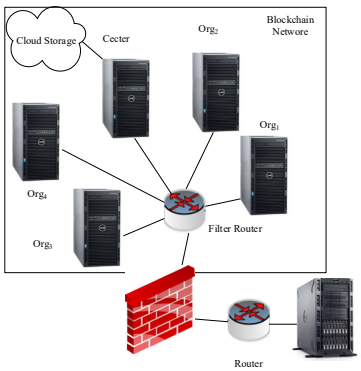

Figure 5. Network topology diagram of distance education system application environment

The proposed method is used to alarm the security threat information under the application network topology environment of the distance education system, and the practical application effect of the technology is analyzed in this paper. Among them, during the operation of the distance education system, there are 20,000 pieces of threat information, including Phishing website URL address, Mobile malicious server IP address, Malicious program file, Malicious email account, DDOS IP, Botnet, Phishing website URL address, and Botnet.

5.2 Data Security Exchange Test of Distance Education System

The single type network behavior data of distance education system belongs to the category of indirect personal information, that is, the single type network behavior data itself does not have the identifiability of user identity, so it is easy to lose in the process of security exchange, and once lost, it cannot be retrieved. Single-type network behavior data in the distance education system usually refers to the teaching file access behavior and interaction behavior of students or teachers in the process of using. The problem with this kind of data is that the data source is single. Under the security threat, once lost, it cannot be retrieved, affecting the normal use of users.

Therefore, the experimental object is the single type network behavior data of the distance education system, and the threshold value is set to 0.08. The proposed method is used to test the percentage of loss of the single type network behavior data when the amount of stored behavior data is different. Results are shown in Figure 6.

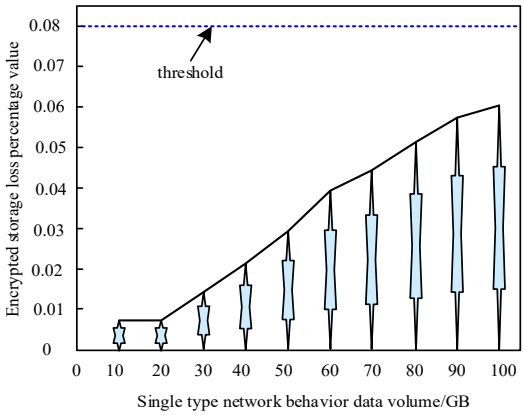

Figure 6. Data security exchange loss percentage of single network behavior

It can be seen from the analysis of Figure 6 that when the proposed technology safely exchanges the single type network behavior data, the percentage of data loss increases with the increase of data volume. Before the single type network behavior data is 20GB, the percentage of loss when the proposed technology safely exchanges single type network behavior data is lower than 0.01. However, with the increase of the amount of single type network behavior data, the percentage of loss of the proposed technology for safe exchange of single type network behavior data shows an upward trend, but the increase is small. When the single type network behavior data is 100GB, the loss percentage value of the proposed technology security exchange single type network behavior data is only about 0.06, which is far below the loss percentage threshold set. The above results show that the technology in this paper has good data security exchange capability of distance education system. The main reason is

that in the process of data exchange, this technology uses RSA symmetric encryption algorithm to reduce the loss of data exchange.

To further verify the ability of the proposed method to safely exchange network behavior data of the distance education system, the data structure transcoding during the safe exchange of network behavior data of the distance education system is used to measure the security exchange ability of the proposed technology. A group of character based distance education system network behavior data is taken as the experimental object, and the transcoding rate is taken as the measurement index. The proposed technology is used to transcode the data structure, and the test results are shown in Figure 7.

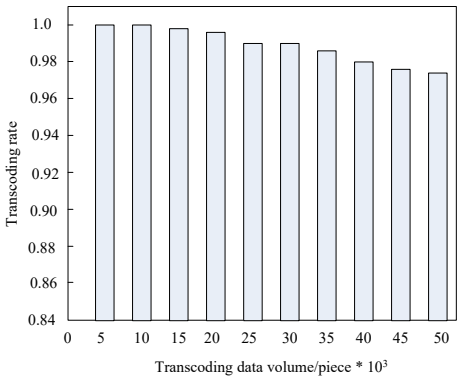

Figure 7. Data transcoding test results

It can be seen from the analysis of Figure 7 that when the proposed technology transcodes the network behavior data of the distance education system, the transcoding rate decreases with the increase of the data volume. When the transcoding data volume is 50 * 10^3, the transcoding rate values are all 1.0. When the amount of transcoding data continues to increase, the transcoding rate of the proposed technology on the network behavior data of the distance education system decreases gradually. When the transcoding data volume is 50 * 10^3, the transcoding rate of the proposed technology for the network behavior data of the distance education system is about 0.97. The above results show that the proposed technology has a high transcoding rate and strong encryption ability for network behavior data of distance education system. It also shows from the side that the proposed technology has an excellent information early warning capability against the security threat of the distance education system.

5.3 Test on Early Warning Capability

First, 10 kinds of network data information of the distance education system are taken as the experimental object, with 1000 pieces of each kind of network information data. During the operation of distance education system, the proposed technology is used to carry out security threat alarm and early warning. The early warning results are shown in Table 2.

Table 2. Network data information security threat alert and early warning results of distance education system

No.	Information type	Level	Early warning
1	Phishing website URL address	5	Accord with
2	Mobile malicious server IP address	5	Accord with
3	-	-	Accord with
4	Malicious program file	4	Accord with
5	Malicious email account	3	Accord with
6	DDOS IP	5	Accord with
7	Botnet	2	Accord with
8	-	-	Accord with
9	Phishing website URL address	5	Accord with
10	Botnet	2	Accord with

As can be seen from Table 2, the proposed technology is consistent with the early warning conditions of the 10 network data information of the distance education system. It shows that the proposed technology can achieve 100% accuracy for the 10 network data information early warning in the distance education system. And from the early warning results, the information type and information early warning level corresponding to the current information serial number can be presented to users, which has a stronger ability to predict the security threat of the education system.

To further verify the security threat information capability of the proposed method, this paper uses the security threat information credibility of early warning as a measurement index. It is used to test the reliability of security threat information when the quantity and type of early-warning security threat information are different. The test results are shown in Table 3.

Table 3. Value of information reliability of early warning security threat

Security threat information quantity/piece	DDOS IP	Phishing website URL address	Mobile malicious server IP address
100	1.0	1.0	1.0
200	1.0	1.0	0.99
300	1.0	0.99	0.99
400	1.0	0.99	0.98
500	1.0	0.99	0.98
600	1.0	0.98	0.98
700	0.99	0.98	0.97
800	0.99	0.97	0.97
900	0.98	0.96	0.97
1000	0.98	0.96	0.97

From the analysis of Table 3, it can be seen that when the number of security threat information of the early warning distance education system increases, the credibility values of different types of security threat information of the proposed technical early warning show a decreasing trend. When the number of security threat information is before 600, the reliability value of the security threat information of the proposed technical early warning DDOS IP type is 1.0. However, when the number of security threat information of URL address of early warning phishing website and IP address of mobile malicious server exceeds 200 and 100, its credibility value shows a downward trend. When the number of security threat information of different types is 1000, the reliability values of security threat information of DDOS IP, phishing website URL, and mobile malicious server IP address types are 0.98, 0.96, and 0.97 respectively. The results show that the reliability values of the security threat information of different types of distance education systems in the technical early warning are high, which can effectively warn the security threat information of different types of distance education systems.

5.4 Test on Early Warning Stability

To facilitate the observation of experimental results, the leader node is manually specified. When the master node is not enabled, the transaction will be sent randomly within 3h to observe the block results of the proposed technology in the early-warning security threat information. When the master node is enabled, the transaction will be sent randomly within 3h to observe the block results of the proposed technology in the early-warning security threat information. The test results are shown in Table 4. When including a subsection you must use, for its heading, small letters, 10pt, left justified, bold, Times New Roman as here.

Table 4. Stability test results of early warning security threat information under different transaction quantities and whether the main node is started

Master node	Group	Number of transactions	Block interval	Average outgoing block interval/s
Not enabled	1	100	5124-5826	63
	2	200	5669-5982	72
	3	300	5799-6003	79
Enable	1	100	5303-5919	51
	2	200	5988-6244	53
	3	300	6157-6556	52

According to the analysis of Table 4, when the master node is not enabled, the more frequent the transaction, the average time between generating blocks slightly increases. When the master node is enabled, the proposed technology keeps the average outbound block interval between 51s and 53s. In summary, there is a small difference in the average blocking interval when warning security threat information, regardless of when the primary node is enabled or not. It shows that the proposed method has good stability in application.

6 Conclusion

Based on the characteristics of block chain, such as open consensus, autonomy, decentralization, distrust, tamper proof, and traceability, this paper has presented a security threat information early warning technology for distance education systems based on block chain. Based on the analysis of the blockchain structure of the security threat information early warning of the distance education system, the technology designs a blockchain-based method for the safe exchange of the distance education behavior data, and optimizes the threat information early warning process. According to the given threat information rating rules, the security threat information warning of distance education systems is realized. This method can provide timely protection and emergency response to promote the sustainable and effective development of the entire threat information ecosystem. The experiment showed that the proposed technology can effectively warn the security threat information of different types of distance education systems, and it had relatively significant application effect and superior stability. It will provide more improvements in related research areas, such as multimodal computing and information fusion [21-22].

Acknowledgements

The paper was funded by National Natural Science Foundation of China with No. 61972104.

References

[1] R. Almesaeed, E. Al-Salem, Sybil attack detection scheme based on channel profile and power regulations in wireless sensor networks, *Wireless Networks*, Vol. 28, No. 4, pp. 1361-1374, May, 2022.

[2] P. Sushma, H. Vajjha, Techniques and Limitations in Securing the Log Files to Enhance Network Security and Monitoring, *Solid State Technology*, Vol. 63, No. 6, pp. 21770-21777, 2020.

[3] D. Wu, A network security posture assessment model based on binary semantic analysis, *Soft Computing*, Vol. 26, No. 20, pp. 10599-10606, October, 2022.

[4] M. Liu, Z. Xue, X. He, J. Chen, Cyberthreat-Intelligence Information Sharing: Enhancing Collaborative Security, *IEEE Consumer Electronics Magazine*, Vol. 8, No. 3, pp. 17-22, May, 2019.

[5] D. Choi, S. Lee, Comparison of Machine Learning Algorithms for Predicting Lane Changing Intent, *International Journal of Automotive Technology*, Vol. 22, No. 2, pp. 507-518, April, 2021.

[6] L. Yang, X. Cao, X. Geng, A novel intelligent assessment method for SCADA information security risk based on causality analysis, *Cluster Computing*, Vol. 22, No. 3, pp. 5491-5503, May, 2019.

[7] M. Ammi, O. Adedugbe, F. M. Alharby, E. Benkhelifa,

Leveraging a cloud-native architecture to enable semantic interconnectedness of data for cyber threat intelligence, *Cluster Computing*, Vol. 25, No. 5, pp. 3629-3640, October, 2022.
[8] R. Riesco, X. Larriva-Novo, V. A. Villagra, Cybersecurity threat intelligence knowledge exchange based on blockchain, *Telecommunication Systems*, Vol. 73, No. 2, pp. 259-288, February, 2020.
[9] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas, Z. H. Abbas, The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges, *Artificial Intelligence Review*, Vol. 55, No. 7, pp. 5215-5261, October, 2022.
[10] R. Vikaliana, R. Rasi, I. N. Pujawan, R. Sham, The Application of Blockchain Technology In Agribusiness Supply Chain Management In Indonesia, *Solid State Technology*, Vol. 63, No. 6, pp. 15644-15657, 2020.
[11] Y. Wang, S. Lin, Research on Security Detection of Computer Blockchain under Eclipse Attack, *Computer Simulation*, Vol. 39, No. 5 pp. 393-397, May, 2022.
[12] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, Y. Park, Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation, *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 8, pp. 8092-8107, August, 2021.
[13] P. Gao, J. Li, S. Liu, An Introduction to Key Technology in Artificial Intelligence and big Data Driven e-Learning and e-Education, *Mobile Networks and Applications*, Vol. 26, No. 5, pp. 2123-2126, October, 2021.
[14] Y. Yuan, J. Zhang, W. Xu, Z. Li, Identity-based public data integrity verification scheme in cloud storage system via blockchain, *The Journal of Supercomputing*, Vol. 78, No. 6, pp. 8509-8530, April, 2022.
[15] V. S. Naresh, V. V. L. D. Allavarpu, S. Reddi, Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN, *The Journal of Supercomputing*, Vol. 78, No. 6, pp. 8708-8732, April, 2022.
[16] Y. Li, J. Zhu, W. Fu, Intelligent Privacy Protection of End User in Long Distance Education, *Mobile Networks and Applications*, Vol. 27, No. 3, pp. 1162-1173, June, 2022.
[17] I. Herrera Montano, J. J. García Aranda, J. Ramos Diaz, S. Molina Cardín, I. de la Torre Díez, J. J. P. C. Rodrigues, Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat, *Cluster Computing*, Vol. 25, No. 6, pp. 4289-4302, December, 2022.
[18] S. Hameed, S. A. Shah, Q. S. Saeed, S. Siddiqui, I. Ali, A. Vedeshin, D. Draheim, A Scalable Key and Trust Management Solution for IoT Sensors Using SDN and Blockchain Technology, *IEEE Sensors Journal*, Vol. 21, No. 6, pp. 8716-8733, March, 2021.
[19] R. Charanya, R. Saravananaguru, Integrity of E-Health Record Ensured With Context-Based Merkle Tree Through Temporal Shadow in Blockchain, *International Journal of Information Technology and Web Engineering*, Vol. 15, No. 4, pp. 72-87, October-December, 2020.
[20] K. Li, Q. Cai, Practical Security of RSA Against NTC-Architecture Quantum Computing Attacks, *International Journal of Theoretical Physics*, Vol. 60, No. 8, pp. 2733-2744, August, 2021.
[21] S. Liu, S. Huang, S. Wang, K. Muhammad, P. Bellavista, J. D. Ser, Visual Tracking in Complex Scenes: A Location Fusion Mechanism Based on the Combination of Multiple Visual Cognition Flows, *Information Fusion*, February, 2023.
[22] S. Liu, P. Gao, Y. Li, W. Fu, W. Ding, Multi-modal fusion network with complementarity and importance for emotion recognition, *Information Sciences*, Vol. 619, pp. 679-694, January, 2023.

Biographies

Zhihua Chen now acts as an Associate Professor at Network Information Center, Guangdong Polytechnic Normal University. He has published about 10 peer-reviewed papers related network quality, network system, and network software on high quality journals.

Gautam Srivastava (SM 19) is currently an associate professor at Brandon University, Canada. He has authored or coauthored a total of 400 papers in conferences or high-status journals and has also delivered invited guest lectures on big data, cloud computing, the Internet of Things, and cryptography. His research is funded by federal grants from the Natural Sciences and Engineering Research Council of Canada and MITACS. His research interests include data mining, big data, and IoT.