Research on the Quality Assessment and Protection of Network Security Body Based on Intelligent Induction and Deep Learning

Yubin Shen*, Hanqing Sun and Miaoxin Li

School of Information Engineering, Henan University of Animal Husbandry and Economy, Zhengzhou 450044, China
E-mail: shenyb716@163.com
**Corresponding Author*

Received 28 January 2024; Accepted 20 August 2024

Abstract

This mechanism mainly saves the induction information in the distributed cloud storage node, and saves the message summary of the induction information in the block chain node, and then the corresponding relationship between the cloud storage node and the block chain node is saved in the induction information management machine. When the user reads the data, the identity authentication is first completed at the induction information management machine, and the induction information is obtained through the key, and finally the data verification is completed at the block chain node. The main advantages of this mechanism are: using block chain to store intelligent sensing information, and using chain storage to reduce the cost of storage, thus enhancing the scalability of block chain storage. This mechanism uses new hash chains to transmit inductive information, thus improving the security of transmission. Through this study proposes an access control strategy for intelligent sensing information. In this way, the user with the key can quickly complete the work certificate and complete the access, while the illegal intruder who does not hold the key cannot calculate the work

Journal of Cyber Security and Mobility, Vol. 13_6, 1283–1304.
doi: 10.13052/jcsm2245-1439.1363

certificate of the next block based on the existing block, so he cannot access the intelligence. Under the network topology set in this paper, the model with step 2 is significantly better than step 1 and 3, with 18.30% and 75.01% reduction on MAPE and 15.66% and 87.79% reduction on RMSE. Through hidden Markov, the security situation of the information system under the time series is determined. Through SSIPN, the security event is not used as a single situation assessment index, but the network topology and node vulnerability are included in the assessment scope to enhance the correlation between the security event and each node in the information system. Based on SSIPN, the weight allocation algorithm of the corresponding nodes is proposed, which accurately reflects the impact of the level of the nodes on the network on the overall situation, and realizes the security situation assessment of the overall network.

Keywords: Intelligent sensing, block chain, access control, data storage, network security.

1 Introduction

Therefore, the Internet of Things can be applied to many intelligent, secure fields, and is an indispensable part, the Internet of Things has been expanding vigorously. Smart can use its connected sensors to personalize its service to users [1, 2]. However, as more and more devices and sensors are connected to intelligence, intelligent systems become more and more complex, and the security of intelligent systems becomes unnegligible at the same time [3, 4]. First of all, intelligent devices have the problems of weak certification ability and low certification performance. Illegal attackers can easily fake user identity and control user devices [5]. Secondly, the smart devices are not safe enough to protect the user's induction data. In addition, data transmission between smart devices has security risks [6]. When the smart device is in an untrusted network, the data transmission of the smart device may be replaced [7, 8]. The traditional intelligent sensing information storage scheme saves all the data in the server cluster, and there are many problems. If you continue to use traditional data storage solutions, it will reduce the efficiency of data access and greatly increase hardware and maintenance costs. On the other hand, when the database cluster fails or is attacked, the sensing information in the intelligence will face the risk of loss [9].

The traditional access control strategy is centralized, by the organization with the server cluster to verify and authorize the identity of users. This way has the disadvantage of low scalability, and easy to cause a single point of failure, easy to lead to the paralysis of the whole system. In addition, there are a large number of privacy information such as user keys and passwords in the traditional access control strategy, if the network attack, will seriously affect the security of access control [10, 11]. Therefore, in order to solve the possible problems in the above intelligence, this paper proposes a safe storage mechanism and access control strategy. The secure storage mechanism solves the problem of low storage capacity of smart devices by keeping the private data of users at the bottom of the chain, and saves the digital summary of the private data in the block chain, so as to improve the efficiency and security of the storage [12]. The access control policy enables the users with the key to quickly complete the access control, and makes the users without the key to complete the creation of the block within a limited time, which is lower than the multiple security attacks [13].

In the Internet of Things field, distributed storage technology is gradually becoming popular. Using distributed technologies such as block chain, combined with edge computing, the storage of its widespread use in transactions involving cryptocurrencies such as Bitcoin. The storage of private data is the most concerned issue for users [14, 15]. Aiming at the problem of private images in cloud storage [16]. A medical data management system that uses smart contracts provided by Ethereum to ensure ownership and data integrity of medical data. Normally, smart contracts automatically execute agreements [17, 18]. In medical treatment, Internet of things and these emerging block chain applications, chain data should be closer to the user, but the existing scheme is difficult to be data in the vicinity of the user and data transmission, in order to cope with these problems, put forward the user as the center of the chain storage scheme, the scheme according to the location of the cache under the chain storage, make the chain data more close to the user, and according to the location and other attributes to determine the user's access rights [19, 20]. Dynamic solutions used by researchers or research partners. In this scheme, the block chain stores the opinions of each research partner.

2 Situation Assessment Technology

2.1 Deep Learning

Intelligence is the control system of smart home, which can control and manage various sensors. After completing the authentication, users can easily operate or monitor smart home appliances through the control center. As shown in Equations (1) and (2).

$$A_{i,j} = P(S_j|S_i), I \leq i, j \leq N \tag{1}$$

$$B_{i,j} = P(O_i|S_j), I \leq i \leq M, I \leq j \leq N \tag{2}$$

Sensors refer to the controlled units in intelligence, including various temperature and humidity sensors, lights, air conditioners, and intelligent switches. Intelligent gateway is the responsibility for information exchange, as shown in Equations (3) and (4), including data transmission between sensors and communication between sensors and server. The server is responsible for business logic, data storage and other functions, including processing inductive information data, providing service interfaces, etc.

$$S_t = f(U \cdot X_{t-l} + W \cdot S_{t-l}) \tag{3}$$

$$f_t = \sigma(W_{xf}x_t + W_{hf}h_{t-l} + W_{cf} * c_{t-l} + b_f) \tag{4}$$

Intelligence is the use of intelligent sensing devices or physical devices to achieve interconnection, while the traditional intelligent sensing devices through the wireless network to obtain data, easy to be malicious attacks or cause data leakage. As shown in Equations (5) and (6), therefore, the security requirements of intelligence can be divided into three layers of models, and the encryption algorithm is the key to determine the security of encryption.

$$i_t = \sigma(W_{xi}x_t + W_{hi}h_{t-l} + W_{cf} * c_{t-l} + b_i) \tag{5}$$

$$c_t = f_t * c_{t-l} + i_t * tanh(W_{xc}x_t + W_{hc}h_{t-l} + b_c) \tag{6}$$

The two classical symmetric encryption algorithms being used today are DES and AES, as shown in Equations (7) and (8), these two symmetric encryption algorithms are an indispensable part of the field of encryption communication. However, the same key in encryption and decryption also becomes a security defect of the symmetric encryption algorithm, because once the key is stolen, the secret text information of the key holder will be easily cracked. Asymmetric encryption algorithm refers to the encryption algorithm using different keys to encrypt and decrypt.

$$o_t = \sigma(W_{xo}x_t + W_{h0}h_{t-l} + W_{c0} * c_{t-l} + b_o) \tag{7}$$

$$h_t = o_t * tanh(c_t) \tag{8}$$

Because of its higher security, the asymmetric encryption algorithm can be well used in the field of identity authentication. The main feature of symmetric encryption algorithm is to use the same key for encryption and decryption. Based on this feature, symmetric encryption algorithm has efficient encryption speed, as shown in Equations (9) and (10), and often it only needs a relatively small amount of calculation to complete encryption and decryption. However, precisely because of this characteristic, the key maintenance cost of the symmetric encryption algorithm is relatively high, which must ensure that the key is not stolen by illegal users. Since this paper mainly involves asymmetric encryption, only a simple introduction to symmetric encryption algorithm.

$$price = price_p + price_\nu * Num * Ratio \tag{9}$$

$$\int cscxdx = ln|cscx - ctgx| + C \tag{10}$$

2.2 Situation Awareness of Network Security

When the device Y needs to transmit encrypted information to device X, it can encrypt the information to be transmitted with the public key of device X and send it to device X, while device X can decrypt the encrypted information sent by the device Y through the saved private key. Asymmetric encryption sacrifices the efficiency of encryption and decryption, increases the computational amount and complexity, but at the same time has higher security and practicality than symmetric encryption algorithm. As shown in Equations (11) and (12), RSA algorithm and ECC are the two most classical encryption algorithms. RSA is one of the most widely used asymmetric encryption algorithms today.

$$Situation_{(t)} = \sum_{i=l}^{n} \left(b_{i,k} * \gamma_i * \left(\sum_{i=l}^{L} I_{(t-i)} \right) \right) \tag{11}$$

$$I_{(t)} = (price_p + price_\nu * Num * Ratio) * situation * level \tag{12}$$

Compared with other asymmetric encryption algorithms, ECC algorithm has higher security and higher efficiency, so ECC algorithm is widely used in different security fields. As shown in Equations (13) and (14), the PoS algorithm gives equivalent interest based on the amount of money you have and the time you have. The more money you hold, the longer you keep it, the more money you gain. PoS is often used for the consensus mechanism of Ethereum.

$$I_{(t+i)} = (price_{\nu} * Num * Ratio) * p * situation * level \tag{13}$$

$$Situation_{network} = log_B \sum_{nodk} \omega_{nodk} * B^I node \tag{14}$$

That is to say, when the more currency the node holds, the larger the equity, the greater the probability of obtaining accounting rights. As shown in Equations (15), (16), the advantage of the PoS algorithm is that it consumes less resources and does not need to spend a lot of time to calculate useless hash values, thus greatly reducing the time spent on the consensus. The disadvantage is that the bookkeeping qualification often falls on the node of holding more money, and can not be completely decentralized. The DPoS algorithm is different from the competition mode between the PoW algorithm and the PoS algorithm, and its miners cooperate with each other to generate blocks.

$$\overline{x} = \frac{l}{n} \sum_{i=l}^{n} x_i \tag{15}$$

$$SD = \sqrt{\frac{\sum_{i=l}^{n} (x_i - \overline{x})^2}{n - l}} \tag{16}$$

There are supernodes in the DPoS algorithm, which are elected by equity holders by voting, and can be generated by completing the responsibility of generating blocks. As shown in Equations (17) and (18), these supernodes are not fixed, and when the supernodes do not fulfill their responsibilities or commit malicious behavior, it will be replaced. The core of DPoS algorithm is the node to run for the block qualification. The more votes the node gets, the easier it is to get the block qualification, which makes the system partially centralized, and thus improves the speed of consensus.

$$x = \frac{x - \overline{x}}{SD} \tag{17}$$

$$\tilde{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{18}$$

The advantages of DPoS algorithm are its higher efficiency and lower operating cost compared with PoS algorithm. The disadvantage is that the algorithm uses a partially decentralized architecture, as shown in Equations (19) and (20), which is easy to monopolize the accounting rights. PBFT algorithm, because in a distributed system, some nodes may be subjected to network attacks and produce malicious behavior, these nodes may affect the stability of the system operation. Distributed systems using the PBFT algorithm can still work properly. Because the PBFT algorithm can solve the problem of data inconsistency in distributed systems such as block chain, and can improve the fault tolerance of the whole system.

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(predict_i - actual_i)^2} \tag{19}$$

$$PoW_j = G_j = \begin{cases} HCN_m, & j = l \\ h_k(h_k(s)|G_{j+l}|), & l > j \geq l \end{cases} \tag{20}$$

3 Network Security Situation Assessment Technology Based on HMMs SIPN

3.1 Evaluation of the Model Design

This strategy mainly consists of the following four algorithms: the message transmission algorithm based on the new hash chain. In this algorithm, the induction information management machine divides the induction information [21, 22]. Secondly, the induction information management machine uses the seed value and each induction information fragment to build the original hash chain. When the element of each hash chain is built, the induction information management opportunity transfers the hash chain element and the encrypted induction information fragment to the cloud storage node [23, 24]. The cloud storage node will use the same seed value and the decryption value to build the verification hash chain. Subsequently, the cloud storage node will judge whether the induction information is tampered with by comparing the verification hash chain between the hash chain and the original hash chain provided by the induction information management machine. Induction information storage algorithm [25, 26]. Then the induction information management machine obtains the induction information from the induction sensor. Figure 1 is a diagram of the adaptive security protection algorithm. Subsequently, the induction information management machine saves the message summary of the induction information in the block chain

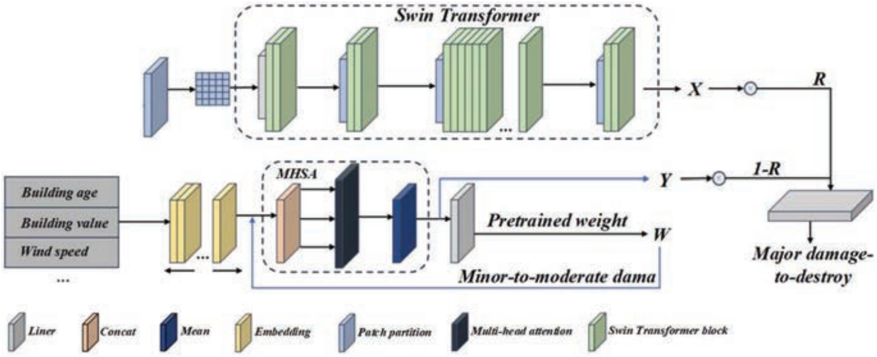

Figure 1 Adaptive security protection algorithm diagram.

storage node. Secondly, the induction information management machine encrypts and transmits the induction information to the cloud storage node. The cloud storage node establishes the induction information database and saves the induction information [27, 28]. Finally, the induction information management machine holds the mapping of the induction information store. Induction information reading algorithm. The user device first completes the identity authentication in the induction information management machine, which obtains the induction information from the cloud storage node according to the sensing information mapping stored by the user [29, 30]. After the cloud storage node accepts the request, they verify the correctness of the induction information from the block chain storage node. And transmit the induction information to the induction information management machine. Induction information validation algorithm.

In this algorithm, after receiving the induction information, the induction information management machine initiates the verification to the corresponding block chain storage node according to the mapping. The block chain storage node verifies the integrity of the induction information after judging the user's signature, and finally returns the verification result. The receiver will also verify the hash chain using the fragments of the received induction information. Once the raw hash chain cannot synchronize with the validation hash chain, the recipient drops the packet and ignores these invalid messages. Therefore, the present mechanism can resist a replay attack. Table 1 for the quantitative results of the sample elements, and in the strategy, induction information management machine, block chain storage nodes, because the induction information is transmitted after divided into multiple segments. As a result, several of the fragments are stolen at the same time. However, in this

Table 1 Sample element quantification results

	Normal Sample	Attack Sample 1	Attack Sample 2
Class	Normal	Port Sweep	Sql Attack
Difficulty Level	/	12	18
Protocol	Tcp	Udp	Icmp
Flag	Sf	S1	S2
Number Of Hotindictors	0	11	6
Type Of Actiyation	0	0.3	0.5
Defense Ability of Destination	0	0.1	0.75
Attack Ratio	/	0.6	0.8

mechanism, the combination order of the induction information fragments is the same as the construction order of the novel hash chain. Since the hash chain is a one-way function, when the illegal user steals the original hash chain IHNi and IHNj and the induction information fragments SIi and SIj, he cannot push back the previous element, so the combined order of the fragments cannot be known. In addition, it is difficult for illegal users to steal all the inductive information fragments at the same time, so this mechanism can resist theft attacks.

3.2 Nodes Weight Assignment Based on SSIPN

In this mechanism, the induction information is stored in the cloud storage node in the form of ciphertext. Without the private key of the cloud storage node cannot be decrypted to obtain the induction information, and the private key will not circulate in the system. At the same time, the induction information is stored in the block chain storage node in the form of a message summary, and the attacker cannot push the induction information backwards through the message summary. In the induction information manager, only the corresponding relationship between the cloud storage node and the block chain storage node is saved, and the attacker cannot obtain useful privacy information. Therefore, the storage of inductive information has a very high privacy. At the same time, the transmission of the induction information is based on the new hash chain, and the unidirectional nature of the new hash chain ensures the privacy of the induction information. Figure 2 shows the anomaly detection algorithm diagram. The access process of the access control strategy based on intelligent sensing information. This section builds a model of the access control strategy.

Access control of intelligent sensing information building algorithm, the accessed edge node EN is saved in the database DBCN. Figure 3 is the

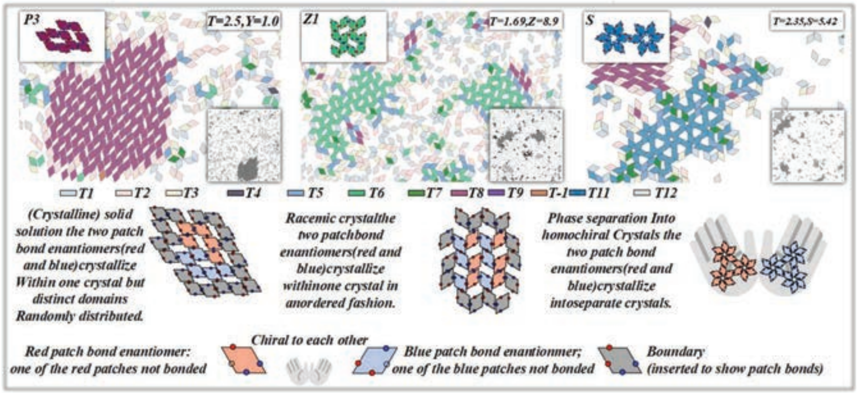
P3
T=2.5,Y=1.0
Z1
T=1.69,Z=8.9
S
T=2.35,S=5.42
T1
T2
T3
T4
T5
T6
T7
T8
T9
T-1
T11
T12
(Crystalline) solid solution the two patch bond enantiomers(red and blue)crystallize Within one crystal but distinct domains Randomly distributed.
Racemic crystalthe two patchbond enantiomers(red and blue)crystallize withinone crystal in anordered fashion.
Phase separation Into homochiral Crystals the two patch bond enantiomers(red and blue)crystallize intoseparate crystals.
Chiral to each other
Red patch bond enantiomer: one of the red patches not bonded
Blue patch bond enantionmer; one of the blue patches not bonded
Boundary (inserted to show patch bonds)

Figure 2 Anomaly detection algorithm.

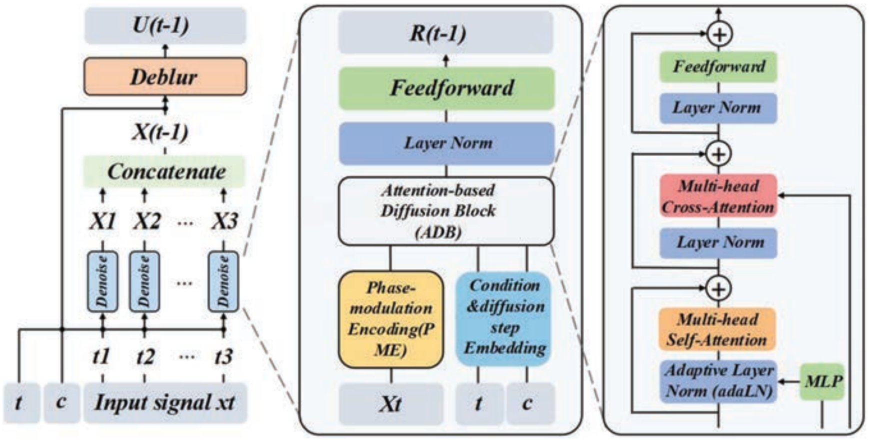
U(t-1)
Deblur
X(t-1)
Concatenate
X1
X2
...
X3
Denoise
Denoise
Denoise
t1
t2
t3
t
c
Input signal xt
R(t-1)
Feedforward
Layer Norm
Attention-based Diffusion Block (ADB)
Phase-modulation Encoding(PME)
Condition &diffusion step Embedding
Xt
t
c
Feedforward
Layer Norm
Multi-head Cross-Attention
Layer Norm
Multi-head Self-Attention
Adaptive Layer Norm (adaLN)
MLP

Figure 3 Training diagram of the deep learning model.

deep learning model training diagram, The model mainly includes objects including users to be visited, user identity sensor, cloud node, edge node, and block chain node. The identity sensor will then be transmitted to the block chain node after the registered user identity is encrypted, and create blocks at the block chain node. After completing the establishment stage of the system, the identity sensor will sense the user to be accessed, and encrypt the identity information of the user to be accessed to the cloud node and the block chain node. Subsequently, the block chain node will solve the proof of work according to the identity information of the user to be visited, and verify the solved proof of work to ensure the legitimacy of the user to be visited.

The blocks are illegally inserted, other block chain nodes can verify the blocks that are newly inserted. When other block chain nodes fail to correctly verify the block, the block is discarded. Forged transactions are generated. First of all, because the key to transaction generation is to the characteristics of the hash chain, the new transactions cannot be pushed back through the existing transactions. It is difficult for the attacker to obtain all the keys at the same time. Using the longest block chain rather than the local block chain for authentication. Therefore, even if the attacker removes the blocks in the local block chain, an impact on the authentication process cannot be achieved, unless the attacker can delete the blocks in all the nodes.

4 Quality Assessment of Network Safety Body Based on Intelligent Induction and Deep Learning

All the transaction information can be verified with the previous transaction information. In this way, the block chain node can judge whether the current block chain is tampered with. block chain node is illegally closed. If the block chain node in the domain is closed, the block chain node is unable to respond. Figure 4 shows the evaluation diagram of malware propagation. Denial of service attack is an illegal attacker malicious occupation of system resources makes users cannot complete access control normally. However, in this policy, the user's access control is realized, which can be directly authenticated according to the block, without requiring the permission of the block chain node. Therefore, when the block chain node is attacked by Dos, the other nodes only need to search for the blocks they need to complete the verification.

A replay attack is achieved by using novel hash chains. During the verification process, each password used is completely different. Rather than

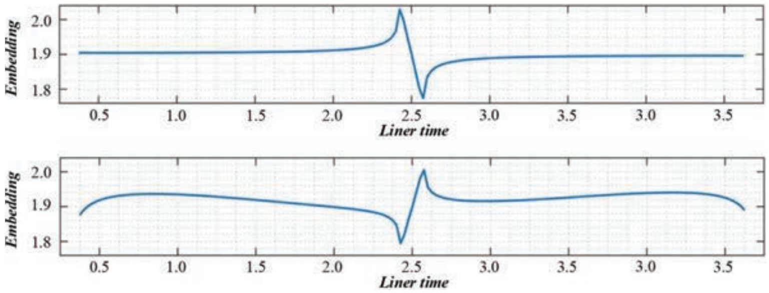

Figure 4 Evaluation diagram of malware propagation.

Table 2 Quantitative table of severity assessment

Grade	Cvss Score Interval
None	0.0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

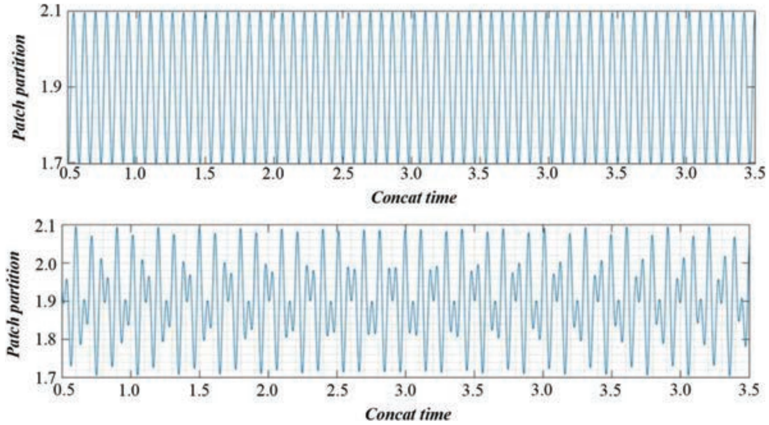

Figure 5 Evaluation diagram of the user behavior pattern.

returning as the verification value for the next access control. Table 2 is the severity rating quantitative table. After receiving the solution, the block chain determines that the solution cannot complete the verification of the solution. The next step is always based on existing attack results, after calculating the reward function, select a node to launch the next attack, While the proposed scalable security event propagation network spreads the effects of attacks, for each diffused node, the situation influence is calculated at the corresponding moment, Computing idea closer to the real situation and situation, and retains the random characteristics of the attack.

The limited polynomial time is the evaluation diagram of user behavior mode. Figure 5 is Evaluation diagram of the user behavior pattern. A fake attack is an illegal attacker forging fake data so that an intelligent sensing device misjudges its identity. A password attack is an illegal attacker who completes access control by guessing the user's password. A central node to ensure that each star node can access each other, when the central node is affected by attack events, it is easy, to the information system the whole network collapse, so in the information network topology of network system in the process of network security situation evaluation, the central node weight proportion should be significantly higher than the weight of the star node. The tree network topology can be understood as multiple star structures, containing multiple central nodes with different degrees of importance. Below the closer to the tree in the structure of the edge of the network topology, the middle part of the tree is equivalent to the information system network layer, the top of the tree is the core of the information system network, through the classification of centralized control mode control the information system, different nodes complete information transmission, the structure of this kind of information system of network security situation assessment, the closer to the top of the node weight should account for higher, the closer to the underlying node weight should account for the lower the proportion.

5 Experimental Analysis

In the course of the understanding of the situation, Designed and implemented the SSIPN, represents each security event occurring on the computer node or on the transmission link and its influencing factors uniformly, and changes the calculation method of the situational impact of the attacker's behavior on the system: in the original Markov game model, Figure 6 shows the evaluation diagram of the malware propagation.

In SSIPN, the nodes have different propagation distances. Figure 7 shows the frequency evaluation diagram of vulnerability utilization frequency. Finally, the log analysis is based on the results of each node in HMM _ SSIPN and the affected nodes of the information system.

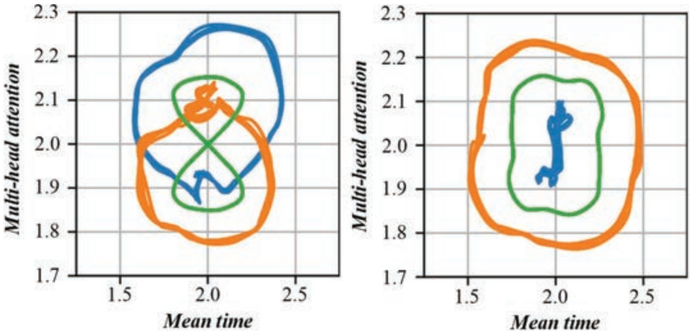

Figure 6 Evaluation diagram of malware propagation.

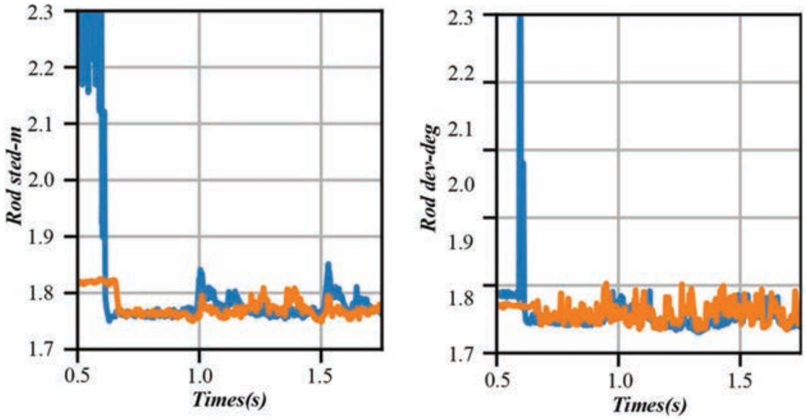

Figure 7 Evaluation diagram of vulnerability utilization frequency.

In this paper, by obtaining the vulnerability, network topology, asset value, extract and select the expansion steps of SSIPN, complete the weight allocation through the network level and the network service, and then use the middle layer to complete the calculation of node and network security situation. Figure 8 shows the evaluation diagram of abnormal detection accuracy. The nodes include servers, routers, terminal devices, etc. The asset value of the node includes the physical value of the node itself, the average value of network services opened by the node, the number of services opened by the node, and the utilization of node service performance. Described by the following formula.

Security events include the security event target node identification, the security event identifier, the vulnerability identification of the security event utilization, and the severity of the security incidents. In the process of network security situation assessment, Figure 9 shows the system response time assessment diagram, and a key step is the node weight allocation. It refers to calculate the contribution and influence of each node to the overall network security situation assessment results according to the value of the security situation under different time periods. In this way.

However, if there is no reasonable node weight allocation process, then there will be deviations and errors in evaluating the overall network security situation only by relying on the security situation of each node in the information system. Therefore, in the network security situation assessment, cannot ignore the node weight allocation of this link. In view of the problem of a large number of security attacks in the intelligent field, Figure 10 is the

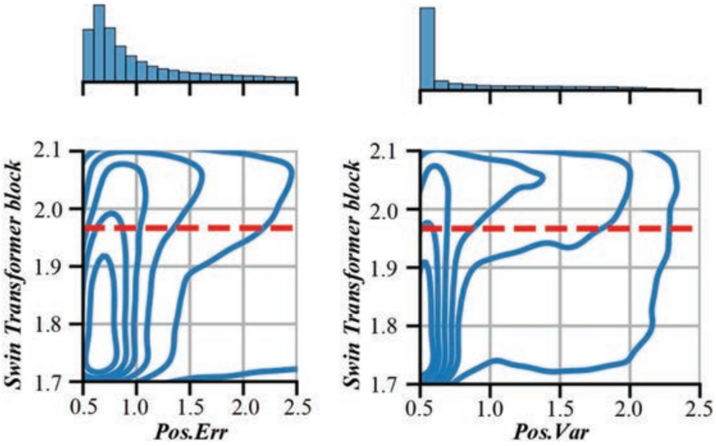

Figure 8 Evaluation plot of anomaly detection accuracy.

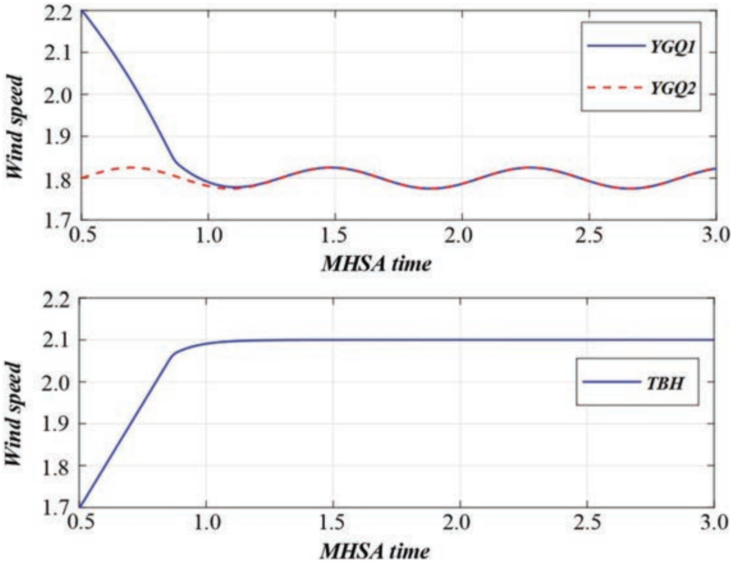

Figure 9 System response time assessment diagram.

evaluation diagram of attack type distribution. This paper proposes an access control strategy for intelligent sensing information. The strategy is mainly divided into four parts.

Figure 11 is the network threat trend assessment diagram. The random value generated by each consensus can be validated by the existing blocks,

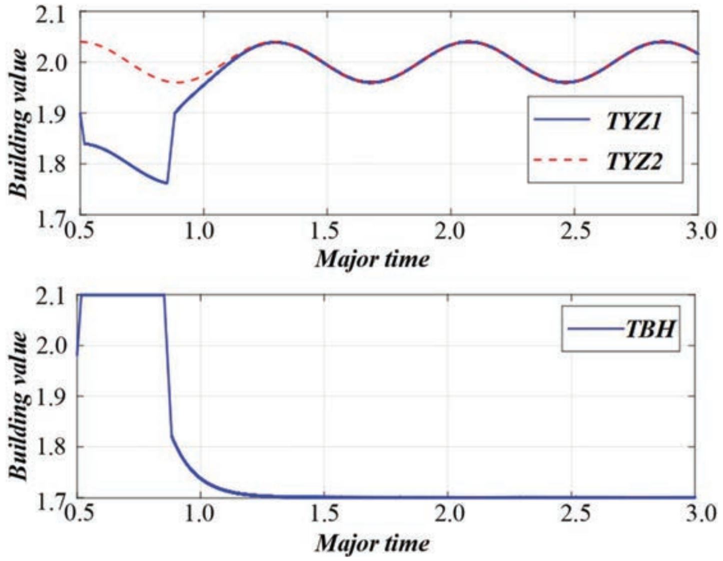

Figure 10 Assessment plot of attack type distribution.

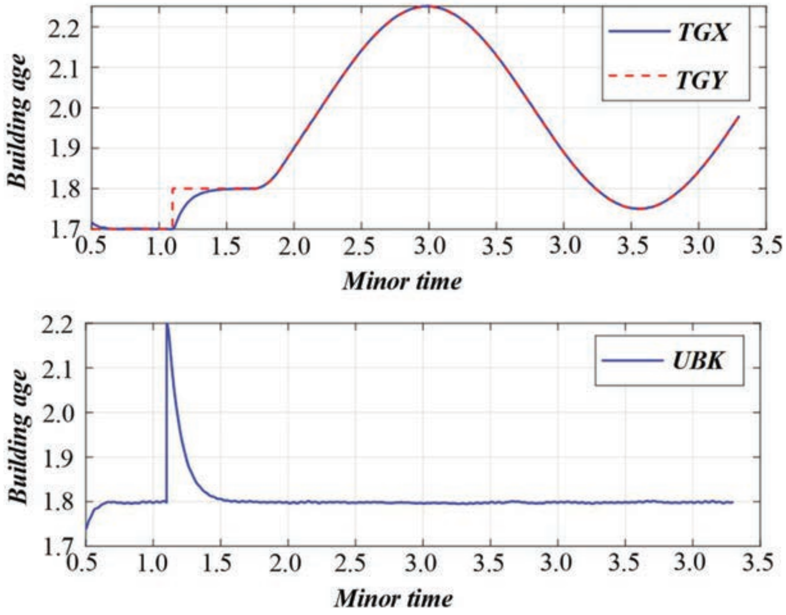

Figure 11 Network threat trend assessment chart.

but the random value of the next consensus cannot be inferred through the existing blocks. Finally, the strategy ensures that only legitimate users can quickly build new hash chains, complete consensus, and ultimately create blocks to complete access control.

6 Conclusion

Research on relevant knowledge in the field of network security situational awareness. It first introduces the relevant technologies and methods of traditional network security defense and points out the shortcomings of this kind of technology, leads to the field of network security situational awareness involved in this paper, and makes a brief overview of the relevant theoretical knowledge in this field. Then we deeply explore the evaluation technology of situation assessment and situation prediction in this field. In terms of situation assessment, it mainly introduces Markov based situation assessment method; in terms of situation prediction, it explores the relevant theoretical knowledge of deep learning, introduces two classical deep learning models RNN and LSTM, and introduces the basic concept of attention mechanism. Build the network security situation assessment model of HMM _ SSIPN. By putting forward the concept of scalable security event propagation network and the node weight allocation method, the design of the situation understanding layer is improved. The evaluation model was then analyzed experimentally to verify the evaluation model by varying the expansion step size of SSIPN. When the ter iterations reaches around 400, the model loss rate gradually completes convergence, with a loss rate of 0.0207. It is smaller than the LSTM and RNN models. We have calculated that the JLSTM model reduces 10.8% from the standard LSTM model and the standard RNN model by 25.5%; 15.6% and 29.9%, respectively. with smaller error and higher stability. Compared with LSTM model and RNN model, it is 10.8% and 25.5% lower, respectively, and 15.6% and 29.9% lower than RMSE, which verifies the accuracy and stability of ILSTM model for network security situation prediction.

Safe storage mechanism induction information storage algorithm, induction information reading algorithm and induction information verification algorithm. The message transmission algorithm based on the new hash chain will divide the induction information into multiple fragments and then encrypt the transmission algorithm, reading algorithm and verification algorithm will save induction information under the chain of cloud storage nodes to improve the scalability of the system, the induction information digital summary saved in block chain to ensure the validation of the system, the induction information correspondence in induction information management machine to ensure the convenience of the user read. According to security analysis and overhead analysis, and can provide users with a safe, efficient and scalable storage mechanism.

Funding

This work was supported by Key Scientific Research Projects of Higher Education Institutions in Henan Province, China (24A413003) and Key Science and Technology Program of Henan Province, China (212102210416).

References

[1] D. Adesina, C. C. Hsieh, Y. E. Sagduyu, and L. J. Qian, “Adversarial Machine Learning in Wireless Communications Using RF Data: A Review,” IEEE Communications Surveys and Tutorials, vol. 25, no. 1, pp. 77–100, 2023.

[2] Y. Afaq and A. Manocha, “Blockchain and Deep Learning Integration for Various Application: A Review,” Journal of Computer Information Systems, vol. 64, no. 1, pp. 92–105, 2024.

[3] G. Agrawal, A. Kaur, and S. Myneni, “A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity,” Electronics, vol. 13, no. 2, pp. 31, 2024.

[4] H. Ahmetoglu and R. Das, “A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions,” Internet of Things, vol. 20, pp. 25, 2022.

[5] O. A. Alimi, K. Ouahada, and A. M. Abu-Mahfouz, “A Review of Machine Learning Approaches to Power System Security and Stability,” IEEE Access, vol. 8, pp. 113512–113531, 2020.

[6] M. A. Amanullah et al., “Deep learning and big data technologies for IoT security,” Computer Communications, vol. 151, pp. 495–517, 2020.

[7] R. Ameri, C. C. Hsu, and S. S. Band, “A systematic review of deep learning approaches for surface defect detection in industrial applications,” Engineering Applications of Artificial Intelligence, vol. 130, pp. 24, 2024.

[8] L. Aversano, M. L. Bernardi, M. Cimitile, and R. Pecori, “A systematic review on Deep Learning approaches for IoT security,” Computer Science Review, vol. 40, pp. 18, 2021.

[9] K. Barik, S. Misra, K. Konar, L. Fernandez-Sanz, and K. Murat, "Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study," Applied Artificial Intelligence, vol. 36, no. 1, pp. 24, 2022.

[10] S. Bharati and P. Podder, "Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions," Security and Communication Networks, vol. 2022, pp. 41, 2022.

[11] E. Btoush, X. J. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A systematic review of literature on credit card cyber fraud detection using machine and deep learning," Peerj Computer Science, vol. 9, pp. 66, 2023.

[12] J. Chen, D. D. Wu, and R. Y. Xie, "Artificial intelligence algorithms for cyberspace security applications: a technological and status review," Frontiers of Information Technology & Electronic Engineering, vol. 24, no. 8, pp. 1117–1142, 2023.

[13] J. R. Cheng, Y. Yang, X. Y. Tang, N. X. Xiong, Y. Zhang, and F. F. Lei, "Generative Adversarial Networks: A Literature Review," Ksii Transactions on Internet and Information Systems, vol. 14, no. 12, pp. 4625–4647, 2020.

[14] D. Dai and S. Boroomand, "A Review of Artificial Intelligence to Enhance the Security of Big Data Systems: State-of-Art, Methodologies, Applications, and Challenges," Archives of Computational Methods in Engineering, vol. 29, no. 2, pp. 1291–1309, 2022.

[15] P. Dixit and S. Silakari, "Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review," Computer Science Review, vol. 39, pp. 15, 2021.

[16] J. Du, Q. Wei, Y. S. Wang, and X. J. Sun, "A Review of Deep Learning-Based Binary Code Similarity Analysis," Electronics, vol. 12, no. 22, pp. 18, 2023.

[17] L. N. Ge, H. A. Li, X. Wang, and Z. Wang, "A review of secure federated learning: Privacy leakage threats, protection technologies, challenges and future directions," Neurocomputing, vol. 561, pp. 18, 2023.

[18] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "Machine Learning and Deep Learning Approaches for CyberSecurity: A Review," IEEE Access, vol. 10, pp. 19572–19585, 2022.

[19] J. Kaur, U. Garg, and G. Bathla, "Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review," Artificial Intelligence Review, vol. 56, no. 11, pp. 12725–12769, 2023.

[20] A. R. Khan, M. Kashif, R. H. Jhaveri, R. Raut, T. Saba, and S. A. Bahaj, “Deep Learning for Intrusion Detection and Security of Internet of Things (IoT): Current Analysis, Challenges, and Possible Solutions,” Security and Communication Networks, vol. 2022, pp. 13, 2022.

[21] G. Kornaros, “Hardware-Assisted Machine Learning in Resource-Constrained IoT Environments for Security: Review and Future Prospective,” IEEE Access, vol. 10, pp. 58603–58622, 2022.

[22] C. Kumar, T. S. Bharati, and S. Prakash, “Online Social Network Security: A Comparative Review Using Machine Learning and Deep Learning,” Neural Processing Letters, vol. 53, no. 1, pp. 843–861, 2021.

[23] B. Lampe and W. Z. Meng, “A survey of deep learning-based intrusion detection in automotive applications,” Expert Systems with Applications, vol. 221, pp. 23, 2023.

[24] J. Lansky et al., “Deep Learning-Based Intrusion Detection Systems: A Systematic Review,” IEEE Access, vol. 9, pp. 101574–101599, 2021.

[25] S. W. Lee et al., “Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review,” Journal of Network and Computer Applications, vol. 187, pp. 22, 2021.

[26] F. C. Liu, M. Li, X. X. Liu, T. Xue, J. Ren, and C. Y. Zhang, “A Review of Federated Meta-Learning and Its Application in Cyberspace Security,” Electronics, vol. 12, no. 15, pp. 35, 2023.

[27] A. Miglani and N. Kumar, “Blockchain management and machine learning adaptation for IoT environment in 5G and beyond networks: A systematic review,” Computer Communications, vol. 178, pp. 37–63, 2021.

[28] S. Najafli, A. T. Haghighat, and B. Karasfi, “Taxonomy of deep learning-based intrusion detection system approaches in fog computing: a systematic review,” Knowledge and Information Systems, vol., pp. 34, 2024.

[29] Z. T. Pritee, M. H. Anik, S. B. Alam, J. R. Jim, M. M. Kabir, and M. F. Mridha, “Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review,” Computers & Security, vol. 140, pp. 21, 2024.

[30] K. Ramezanpour and J. Jagannath, “Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN,” Computer Networks, vol. 217, pp. 11, 2022.

Biographies

Yubin Shen was born in Jiaozuo, Henan, P.R. China, in 1976, received his M.Sc. degree in 2005 from Southwest University of Science and Technology, P.R. China. Now he is a lecturer in School of Information Engineering, Henan University of Animal Husbandry and Economy. His main research interest include Networked control system, communication security, robust control, intelligent control.

Hanqing Sun was born in Xinxiang, Henan, P.R. China, in 1981. He received M.Sc. degree in 2005 from Zhengzhou University, P.R. China. Now he is a lecturer in School of Information Engineering, Henan University of Animal Husbandry and Economy. His main research areas are network information, communication security, and traffic prediction.

Miaoxin Li was born in Lushan, Henan, P.R. China, in 1988. She received M.Sc. degree in 2018 from Huaqiao University, P.R. China. Now he is a lecturer in School of Information Engineering, Henan University of Animal Husbandry and Economy. His main research areas are network information, communication security, and traffic prediction.