Research on Cybersecurity Talent Assessment Model Based on Blockchain Technology and Neural Network

Jun Zhao*, Chen Zhou[a]

National intelligent society comprehensive governance experimental base (CUIT Shuangliu Industrial College), Chengdu, China, Chengdu University of Information Technology Chengdu, China

*zhaojun@cuit.edu.cn, [a]352029430@qq.com

Abstract. This paper proposes a cybersecurity talent assessment model based on blockchain and neural network, aiming to realize comprehensive, efficient and secure supervision of cybersecurity talents. The model is centered on blockchain technology, and a secure and trustworthy cybersecurity talent information base is constructed using a federation chain. The traditional DPoS consensus mechanism is improved and a neural network algorithm is introduced for evaluating and predicting the ability, behavior, and reputation of talents to provide a scientific basis for regulation. The experimental results for the improved consensus mechanism and neural network show that the model is able to realize comprehensive supervision of cybersecurity talents, improve the efficiency and accuracy of supervision, and provide strong support for the cultivation and management of cybersecurity talents.

Keywords: blockchain； neural network； cybersecurity talent； consensus mechanisms

1 Introduction

With the rapid development of information technology, the problem of network security has become the focus of global attention[1]. Strengthening the cultivation and team building of network security talents has become an indispensable part of the high-quality development of China's talent pool[2]. However, the traditional way of regulating cybersecurity talents often suffers from inefficiency, easy tampering of data, and insufficient security. We propose a cybersecurity talent assessment model based on blockchain and neural network, aiming to solve the problems of traditional regulatory approaches. The model combines the tamperability of blockchain technology with the intelligent analysis capability of neural network technology to achieve comprehensive, efficient, and secure regulation of cybersecurity talents. First, blockchain technology is used to build a decentralized and distributed data storage and access platform to ensure the security and trustworthiness of talent data; at the same time, intelligent analysis and risk assessment of cybersecurity events are conducted through neural network models to provide strong support for regulatory decision-making. Our proposed cybersecurity

E. P. H. Lau et al. (eds.), *Proceedings of the 2024 3rd International Conference on Information Economy, Data Modelling and Cloud Computing (ICIDC 2024)*, Advances in Computer Science Research 114,
https://doi.org/10.2991/978-94-6463-504-1_25

talent assessment model based on blockchain and neural network not only improves regulatory efficiency and data security, but also provides new ideas and methods for cybersecurity talent training, certification, and regulation.

2 Relevant Theories and Research Significance

2.1 Overview of Blockchain Technology and Neural Networks

The core of blockchain lies in its distributed ledger technology, which has been refined and developed to form the underlying framework of distributed applications, with decentralization, transparency and tamper[3]. Which incorporates consensus, encryption, digital signatures, hashing, and economics reward mechanisms to write blocks of data into a chained ledger for the purpose of decentralization as an innovative technology. Since the blockchain system is a decentralized system[4], for the integrated system to operate efficiently, a consensus mechanism is necessary to reach a consensus among the various individuals involved in the transaction. The consensus mechanism allows for the consensus of each node to be reached and ensures the consistency and stability of the data storage.

With the advent of the era of big data, artificial intelligence has become the focus of attention in all walks of life, especially Artificial Neural Network (ANN), which occupies a pivotal position in artificial intelligence applications[5]. It effectively models and deeply analyzes complex data by simulating the information transfer between neurons and the internal processing mechanisms, thus revealing the intrinsic patterns and characteristics of the data. With its unique distributed information storage, efficient parallel processing capability, and excellent self-learning ability, neural network is able to deeply discover the intrinsic laws of things based on the established evaluation criteria, processes, and training samples[6]. Through continuous learning and fine adjustment of weights, the neural network is able to accurately capture the intricate and complex internal relationship between evaluation indicators and evaluation levels, thus providing a comprehensive and objective integrated evaluation for each talent and ensuring that the evaluation results are fair and reasonable.

2.2 Significance of the Research

The traditional way of talent database construction is not suitable for the current environment, government departments, companies, enterprises, efficient and other units of the demand is difficult to unify, the quality of the submitted data is difficult to guarantee, etc. are the challenges faced. And most importantly, most of the talent database by a single organization for centralized management, data security risks increase.

Blockchain technology, on the other hand, provides a good solution. Using blockchain technology to build a cybersecurity professional talent pool has the following advantages. First, blockchain, with its decentralization and data tampering characteristics, provides a highly reliable data storage and verification mechanism for the qualification, training, certification and other information of cybersecurity talents, reduces the risk of a single point of failure, and improves the robustness of the system. Second, the

asymmetric encryption algorithm used in the blockchain provides strong security for data storage in the database. Third, the smart contract can automatically execute the processes of qualification and training and certification of cybersecurity talents, which increases the automation level of the system and reduces the burden and cost of manpower.

Cybersecurity talents as a large number of groups, the data complexity in the database is quite high, the use of neural networks as an auxiliary tool for the identification, screening and evaluation of talents is a program with considerable advantages. Neural networks are trained to accurately recognize the criteria and categories of various talents and predict potential threats, providing accurate data support for the regulation of cybersecurity talents.

3 Model Implementation

3.1 Node Analysis

The users in this model are mainly of the following types: cybersecurity talents, university organizations, enterprises and government units. As in the ordinary model, each user can perform operations such as querying and modifying their own basic information.

In the model, when university institutions, enterprises and government units need to upload information about cybersecurity talents, i.e., add new nodes to the blockchain of the corresponding cybersecurity talents. We have classified them into non-mandatory and mandatory operations, for adding common information, i.e., non-mandatory operations require authorization from the talent. For certain information, such as a university institution wanting to upload the talent's disciplinary information into the model, authorization is not required. This more flexible authorization mechanism improves the efficiency of the model and ensures the stability of the model.

3.2 Block Node Design

We designed and implemented our blockchain structure by modifying it on top of the traditional blockchain data structure, as shown in Table 1. Each block consists of three parts: block header, data and metadata.

Four fields are stored in the block header (Header), where the ID field stores the ID number of the cybersecurity talent, which facilitates the query and retrieval of the talent due to the uniqueness of the ID number. Then there is the data hash value of the parent block and the new block, and we use the SHA-256 algorithm[7] to generate the hash value. Finally, the account information of the adders.

The Data section is used to store timestamps, information about cybersecurity talents, and signature information of the adders. Among them, the information of cybersecurity talents comes from the academic information added by colleges and universities, and the employment information added by enterprises and government units. In order to prevent the data from being maliciously tampered with and falsified, the adders must store their signature information as well.

Table 1. Block structure

Block structure	Field	Details
Block header (Header)	ID	Identity card number of the talent
	ParentHashCode	The data hash of the parent block
	HashCode	The data hash of the new block
	TinID	Addressee account information
Data (Data)	Timestamp	timestamp information
	DataText	Information on Talent
	Signatures	Signature information of the person who added it
Metadata (MataData)	Times	Number of times block information is added
	Base	Basic Information on Talents

MetaData (MetaData) mainly stores the number of times the block has been added and the basic information of the talent, and the basic information of the cybersecurity talent includes name, gender, and place of origin.

3.3 Talent Assessment

We categorize the information about each cybersecurity talent into static and dynamic information. Static information is the personal or professional attributes of the talent that do not change or change slowly over time, including educational background, work experience, skills and knowledge, and personal traits. Dynamic information, on the other hand, refers to personal realizations or behaviors that change with time and mood, including job performance, training and development, project contribution, and emergency response. The detailed categories are shown in Table 2.

Since we categorized the information of cybersecurity talents into static and dynamic information, and the learning ability of a single neural network model is limited, we constructed two independent structure-aware attention neural networks[8], which are used to learn the static and dynamic information of talents respectively.

We constructed a structure-aware attention neural network assessment model[8] for comprehensive assessment and risk prediction of talents. As shown in Fig. 1, the static and dynamic information of cybersecurity talents are input into two structure-aware attention neural network models, i.e., the static information model and the dynamic information model, respectively. These two models can analyze and evaluate the two different kinds of information individually. In order to make the final results more objective and realistic, we input the outputs of the static and dynamic information models together into the global model, which outputs the final results.

In the static and dynamic information models, we use the following formulas to process the input features and generate assessment results. First we vectorize the input talent information with features, represented as a high-dimensional vector:

$$F_S = \{f_1^s, f_2^s, f_3^s, f_4^s\} \quad (1)$$

$$F_D = \{f_1^d, f_2^d, f_3^d, f_4^d\} \quad (2)$$

Where $f_1^s, f_2^s, f_3^s, f_4^s$ denote the embedding vectors of educational background, work experience, skills and knowledge, and personal attributes in static information, and $f_1^d, f_2^d, f_3^d, f_4^d$ denote the embedding vectors of job performance, training and development, program contribution, and emergency response in dynamic information, respectively. Then the importance weights of each feature are calculated separately by the attention mechanism[9]:

$$\mathrm{A} = \mathrm{softmax}(\mathrm{QK}^t/\sqrt{d_k}) \tag{3}$$

Where Q is the matrix of the query, K is the key matrix and d_k is the dimension of the feature vector. The features are then weighted and summed according to the attention weights and the resulting composite feature representation is:

$$\mathrm{H} = \mathrm{AV} \tag{4}$$

Where V is the value matrix and H is the integrated feature representation. Finally, the corresponding evaluation results are generated by fully connected layers and activation functions:

$$\mathrm{Y} = \sigma(\mathrm{WH} + b) \tag{5}$$

Where W is the weight matrix, b is the bias term, σ is the activation function, and Y is the evaluation result. We input the results of the dynamic and static model outputs into the global model and predict the final result by calculating the following formula:

$$Y_G = (\theta_1, \theta_2, \theta_3, \theta_4)Y_D + (\mu_1, \mu_2, \mu_3, \mu_4)Y_S + \beta \tag{6}$$

Where Y_G denotes the predicted output results of the global model output, Y_D and Y_S are the assessment results of the dynamic and static models, $\theta_1, \theta_2, \theta_3, \theta_4$ and $\mu_1, \mu_2, \mu_3, \mu_4$ are the learnable weight parameters, and β is the bias term, respectively. The assessment results output from the model include the following information: (1) Comprehensive score, which derives the overall score of cybersecurity talents based on the comprehensive assessment of input features. (2) Risk prediction, the prediction of the potential risks of the talent, including possible violation risks and career risks. (3) Strengths analysis, assessing the talent's strengths in terms of education, work experience, and honor information. (4) Improvement suggestions, which are given based on the assessment results to help talents improve their competitiveness.

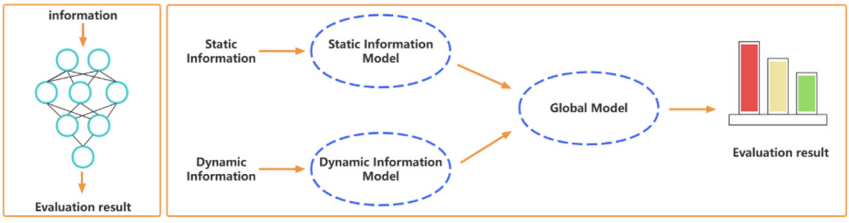

Fig. 1. Structure of the assessment model

Table 2. Cybersecurity Talent Information Category

Categories	Categories	Categories
Static Information	Educational Background	Education: Bachelor's, Master's, Doctorate Specialization: Computer Science and Technology, Network Security, etc. Academic achievements: GPA, publications, etc. Training organization certification: Cisco, CISSP, etc.
	Working Experience	Industry experience: number of years, specific position, type of company worked for Project experience: number of projects, size, results of parameters Job changes: from junior to senior positions
	Skills and Knowledge	Programming languages: Python, Java, C++, etc. Network security technology: firewall, intrusion detection, encryption technology, etc. Knowledge of tools and software: Nmap, Wireshark, etc.
	Attitude	Motivation and interest: passion for the profession, personal career plans Personality traits: responsibility, patience, stress tolerance Values: ethical standards, professional ethics
Dynamic Information	Working Performance	Mandate delivery: punctuality, quality, innovation Teamwork: ability to communicate and collaborate with coworkers Problem-solving skills: coping strategies and outcomes in the face of challenges
	Training and Development	Training activities participated in: online courses, seminars, workshops, etc. Skill enhancement: learning new skills, deepening old skills Career development: promotion, job-hopping, adjustment of career plans
	Project Contribution	Project roles: leadership, execution, support, etc. Contribution: workload, innovation, impact, etc. Feedback and evaluation: from coworkers, supervisors, customers
	Emergency Response	Speed and Efficiency in Responding to Cyber Attacks Creativity and effectiveness of solutions After-action review and improvement

3.4 Consensus Mechanisms

In a distributed computing environment, blockchain technology establishes a foundation of trust between unknown peers. In order to verify the legitimacy of transactions, consensus algorithms are widely used[10]. In traditional blockchain, the consensus mechanism mainly realizes competition through users' Proof of Work (PoW) or Proof

of Stake (PoS) to elect the bookkeeper. However, these mechanisms are usually accompanied by high computational costs and resource consumption, which are not conducive to the lightweight and efficient operation of the system.

We have improved the traditional Delegated Proof of Stake (DPoS) mechanism as the consensus mechanism in our model. In the traditional DPoS mechanism, a number of bookkeeping nodes are elected by the users to form a board of directors by voting to represent the users in bookkeeping. However, such an election method is not efficient in the case of a large number of nodes.

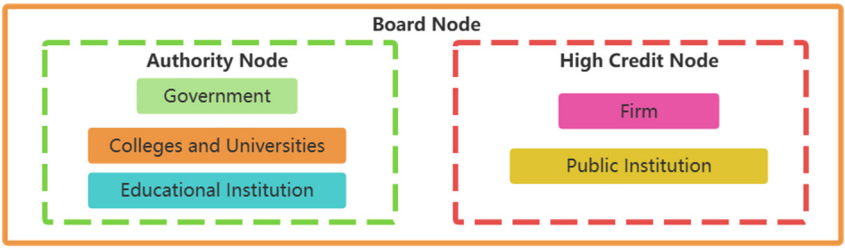

Fig. 2. Improved DPoS board node composition

Table 3. Credit evaluation indicators for enterprises and institutions

Norm	Details
Talent pool	Proportion of talented people in a business or organization to the total number of employees
Technical level	Number of technology patents granted to enterprises or institutions
Academic level	Number of academic papers published by enterprises or institutions
Professional level	The size of the business of the enterprise or institution
Financial level	Asset size and debt ratios of the enterprise or utility
Activity level	Number of businesses or institutions involved in bookkeeping
Experience with awards and penalties	Number of rewards and penalties received

As shown in Fig. 2, the users in our system consist of universities, educational institutions, government, enterprises and utilities. We specify the nodes of universities, educational institutions and government as authority nodes and these nodes occupy 15% of all nodes and the remaining 75% of nodes consist of enterprises and utilities. We select a group of nodes with the highest credit from the corporate and institutional nodes along with the authoritative nodes to form the board of directors in DPoS, and the number of these nodes occupies 30% of all the nodes. The nodes in the board of directors must have the approval of more than half of the board of directors nodes in order to be successful in their bookkeeping. We use a total of seven metrics, namely, talent pool, technology level, academic level, business level, financial level, activity level, and reward and punishment experience, to measure the creditworthiness of a company or an organization, and the detailed information is shown in Table 3.

4 Experiments

4.1 Consensus Mechanism Testing

To highlight the superiority of our consensus mechanism, we tested its election time, i.e., the time required to elect all the board nodes. We constructed five federated chain networks containing universities, governments, educational structures, institutions, and enterprises, with the number of nodes in the five networks being 200, 300, 400, 500, and 800, respectively. We conducted 10,000 tests using the traditional DPoS mechanism and our improved DPoS mechanism, respectively. The results of the tests are shown in Fig. 3, where our consensus mechanism reduces the election time by 35% relative to the traditional DPoS mechanism.

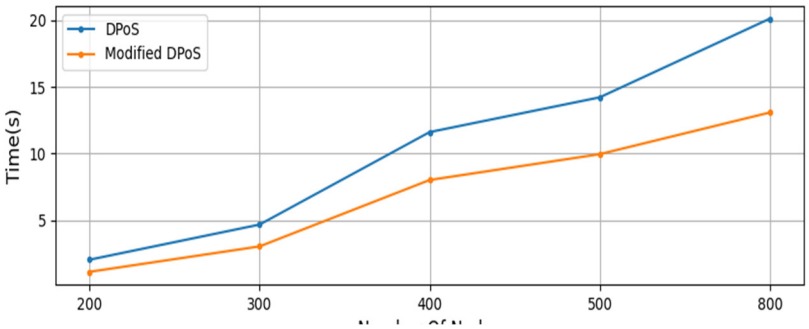

Fig. 3. Election speed testing results

4.2 Talent Assessment Testing

In order to validate the accuracy of our model for talent assessment, we collected information on 12634 cybersecurity professionals and made a dataset, which contains different academic degrees, work experiences and project experiences. We first manually specify the corresponding evaluation scores of these talents, and then divide them into training and testing sets with a ratio of 4:1. During testing, we specify that as long as the output of the model differs from the predetermined results by less than 5%, the results are acceptable. As shown in Table 4, our model achieved excellent results for all four predicted outcomes.

Table 4. Talent assessment testing results

Categories	Accuracy
Comprehensive Score	95.33%
Risk Prediction	93.51%
Strengths Analysis	98.68%
Improvement Suggestions	91.35%

5 Conclusion

Our proposed cybersecurity talent assessment model based on blockchain and neural network provides a brand new solution for the regulation and management of cybersecurity talents by combining the decentralization and tamperability of blockchain technology and the intelligent analysis capability of neural network technology. Experimental results show that our model is comparatively and substantially ahead of the traditional consensus mechanism in terms of its efficiency, and is able to accurately assess and analyze talent information. The model not only ensures the integrity and security of data, but also improves the efficiency and transparency of regulation, which is of great significance for promoting the healthy development of cybersecurity talent market.

References

1. Liu J, Su PR, Yang M, He L, Zhang Y, Zhu XY, Lin HM. Software and Cyber Security-A Survey[J]. Journal of Software, 2018, 29(1): 42-68(in Chinese).http://www.jos.org.cn/1000-9825/5320.htm
2. Qian ZHOU, Haiping HUANG, Le WANG, Yanchun ZHANG, Fu XIAO. Connotation and practice of the integration of academic field based on Bourdieu's theory——taking the cultivation of cyberspace security talents as an example[J]. Chinese Journal of Network and Information Security, 2023, 9(4): 178-187.
3. L. Alashaikh, "Blockchain-Based Software Systems: Taxonomy Development," 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 2021, pp. 491-498, doi: 10.1109/Blockchain53845.2021.00075.
4. Xie QQ, Dong F. Survey on Lightweight Blockchain Technology. Journal of Software, 2023, 34(1): 33-49(in Chinese). http://www.jos.org.cn/1000-9825/6421.htm
5. Z. Faris and I. A. Murdas, "A Comparative Study between Artificial Neural Networks and Optical Neural Networks," 2022 4th International Conference on Current Research in Engineering and Science Applications (ICCRESA), Baghdad, Iraq, 2022, pp. 143-147, doi: 10.1109/ICCRESA57091.2022.10352460.
6. Zhang ZK, Pang WG, Xie WJ, Lü MS, Wang Y. Deep Learning for Real-time Applications: A Survey[J]. Journal of Software, 2020, 31(9): 2654-2677(in Chinese). http://www.jos.org.cn/1000-9825/5946.htm
7. Guoqiang GAO,Zichen LI. Research and design of authenticated encryption algorithm based on AES round function[J]. Chinese Journal of Network and Information Security, 2020, 6(2): 106-115.
8. Sun, Y., Zhuang, F., Zhu, H. et al. Market-oriented job skill valuation with cooperative composition neural network. Nat Commun 12, 1992 (2021).
9. VASWANI A, SHAZEER N, PARMAR N, et al. Attention is All you Need[J]. Neural Information Processing Systems,Neural Information Processing Systems, 2017.
10. A. Endurthi and A. Khare, "Two-Tiered Consensus Mechanism Based on Proof of Work and Proof of Stake," 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 349-353, doi: 10.23919/INDIACom54597.2022.9763215.