Information Sharing Security Protection System Based on Artificial Intelligence

1st Yawen Mi
College of Basic Military and Political Education
National University of Defense Technology
Changsha, China
miyawen624@126.com

2nd Enduo Gao
School of Physics and Electronics
Central South University
Changsha, China
1263551501@qq.com

2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC) | 978-1-6654-9111-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICMNWC56175.2022.10031986

Abstract—**As the problem of information sharing security becomes more and more serious and network attacks are constantly defended, the protection techniques used to solve the information sharing security problem must be constantly updated. In order to address the shortcomings of existing research on information sharing security protection, this paper briefly discusses the test environment and parameter configuration of the protection system proposed in this paper, based on the functional equations of recurrent neural networks and the elements of information sharing security. The software structure and function of the protection system using recurrent neural networks are also discussed, and the designed information sharing security protection system is finally applied to information misuse (IM) and information anomaly (IA) and security response (SR) for experimental testing. The experimental data show that the accuracy of the protection detection for information misuse (IM) reaches about 97.5 on average among all information samples. The accuracy of the protection detection of information anomaly (IA) reaches about 97.2 on average. The accuracy rate of security response (SR) protection detection reaches 96.7% on average. Therefore, it is verified that the information sharing security protection system designed in this paper has good protection effect.**

Keywords—artificial intelligence, information sharing, security protection, neural network.

I. Introduction

With the gradual popularization of computer technology. In a variety of information exchange and sharing environment, each user's life is becoming more and more convenient, bringing a large number of network security problems, information security and privacy protection has ushered in new challenges.

Nowadays, more and more scholars have conducted a lot of research on information sharing security protection system through various technologies and system tools, and have also achieved certain research results through practical research. El-Latif AA believes that the threat of online information sharing has become a concern of various fields and sectors. While there are many existing countermeasures, one that is commonly used among cybersecurity professionals in various fields and sectors is cybersecurity threat response. This approach refers to any information that identifies, evaluates, detects, and responds to threats to information sharing through network information. It includes indicators of threats, methods of threats, and procedures. CTI sharing is considered as a scientific method to improve the security protection capability of information sharing [1]. Romansky R P In order to develop and practice information sharing and security protection systems in the network, scientific and effective protection protocols and procedures are needed. Romansky R P proposes two approaches based on the assumptions of algorithms and protection systems. But there is one most vulnerable link in network password parsing. The sensitivity and controllability of the initial information parameters can theoretically provide a larger key space for the protection of known attacks. Romansky RP proposes a scientific information sharing security protection mechanism based on QWs. Then perform performance analysis, and experiments show that the proposed method has high security and high stability in network information sharing [2]. The goal of Haque S research is to provide a reliable protection environment to ensure network information security. Due to the complexity of network information, putting security information in the cloud has become a monitoring standard through certain information monitoring methods. Under various conditions, these information security issues involve the transfer of information to the cloud, and a method is proposed to enable the transfer of personal information to the cloud and to limit the threats of such information from entering the cloud environment. The information transmitted to the cloud should be detected to protect the user's information, and the risks and protection techniques of network information are listed [3]. Although the existing research on aviation control safety risk assessment system is very rich, the research on aviation control safety risk assessment system based on AHP still has certain limitations.

Therefore, in order to enrich the existing research in information sharing security protection system, this paper firstly introduces the concept of recurrent neural network functional equations and the application of artificial intelligence technology as well as the elements of information sharing security, secondly discusses the test environment and parameter configuration of the information sharing security protection system proposed in this paper, and finally conducts experimental tests by applying the designed information sharing security protection system structure specifically to information misuse (IM) and information anomaly (IA) and security response (SR), and finally experiments show the effectiveness of the information sharing security protection system designed in this paper.

II. Information Sharing Security Protection Based on ArtificiaIl ntelligence

A. Artificial Intelligence Technology

The use of artificial intelligence techniques in this information sharing security protection [4].

1) Establish a rule-producing expert system: This system refers to a detection system with rich experience of experts. Managers can compile standards from the intrusion situation and identify the security degree coefficient of the system by using the detection function of the system [5].

978-1-6654-9111-2/22/$31.00 ©2022 IEEE

2) Artificial neural network system: The research and development of this system is a learning skill formed by an efficient scientific research team in the long-term simulation of the human brain. In addition to the above-mentioned favorable conditions, it also has good learning ability and adaptive ability to realize rapid identification of intrusion situations [6].

3) Artificial immunization technology: The principle of this technology is based on the human immune system, and the human body can make a self-protection phenomenon against the external environment and train it through information security technology [7].

B. Information Sharing Security

Elements of Information Sharing Security

1) Information assets: Information includes all forms of data, documents, information, etc. Information assets refer to information that has value to an organization and is stored in any way [8].

2) Security risks: Information assets face many security threats, such as information misuse, abnormal information, etc. Due to the existence of some weak links that can be used or destroyed, information assets may suffer losses [9].

3) Vulnerability: refers to the weak link that may be exploited by threats and cause damage to assets. These vulnerabilities may exist in software, hardware, workflow, personnel, etc. [10].

C. Recurrent Neural Networks

According to the information state output by the previous recurrent network unit and the input of the current recurrent network unit, the forget gate jointly controls how much information of the monitoring state of the previous recurrent network unit needs to be protected, that is, the information output by the previous recurrent network unit is proportionally adjusted [11]. Its specific formula is as follows:

$$k_x = \vartheta(R_k \cdot [t_{x-1}, u_x] + c_k) \qquad (1)$$

$$\widehat{m} = k_x * a_{x-1} \qquad (2)$$

Among them, R_k is the weight matrix of information sharing security protection, t_{x-1} , u_x represents the combination of the protection state t_{x-1} of the previous information and the input information u_x of the current protection, c_k is the information abnormality, and ϑ is the classification activation function. This function can map $(-\infty, \infty)$ to (0,10), so the value of k_x is between 0 and 10, so that the detection rate of the protection state of the previous information entering the current protection state can be adjusted.

Information sharing security protection needs to first calculate the protection state $\widehat{m}_x$ of the current information, which determines what kind of new information needs to be detected into the security protection state in the current security protection. Its calculation formula is:

$$\bar{m} = tan\square(R_m \cdot [t_{x-1}, u_x] + c_m) \qquad (3)$$

Among them, R_m is the weight matrix of information sharing security protection, c_m is the information anomaly, and tanh is the activation function commonly used in recurrent networks.

III. Investigation and Research on Information Sharing Security Protection System Based on Artificial Intelligence

A. AI-Based Information Sharing Security Protection System Test Environment

1) Hardware environment

a) *Monitoring host (Web server):* Pentium(R) Dual-CoreCPUE54002.70G, 2G memory, 320G hard disk server host

b) *Control terminal:* Pentium(R) Dual-CoreCPUE53002.60GHz, 1G memory, 250G hard disk.

2) Software environment

a) Operating system: The monitoring web server adopts Windows Server 2003 SP2 operating system.

b) *Control terminal:* using WindowsXPSP3 operating system website server software: IIS6.0.3.

3) Network environment

a) Network type: LAN.

b) Network bandwidth: 100M.

c) Network card speed: 10/100M.

B. Parameter Configuration of Information Sharing Security Protection System Based on Artificial Intelligence

In this paper, different information sharing security protection parameters are used in the experimental test. Users can add information sharing security protection objects and set related information sharing security protection parameters on the front-end page of the system by logging in through a browser. To add the information sharing security protection object, the name, IP address and group word of the relevant network should be filled in, while the information sharing security protection parameters can be configured according to the user's business requirements and the actual situation of the system. The specific parameter configuration is shown in Table I:

TABLE I. INFORMATION SHARING SECURITY PROTECTION OBJECT PARAMETERS

Protection category	Protective parameters
The server	Network ID, interval, IP address, performance indicator threshold
The middleware	Network ID, network type, time interval, port number, network version
The database	Network ID, information base type, user name and password, and counter threshold
Network equipment	Network ID, network type, IP address, interval, performance indicator threshold

IV. Application Research of Information Sharing Security Protection System Based on Artificial Intelligence

A. *Software Structure Design of Information Sharing Security Protection System Based on Artificial intelligIce*

In this paper, the software development of information sharing security protection system is based on Linux environment, and QT is used as the development tool. The software structure of information sharing security protection system is designed, which mainly includes three modules: input layer, hidden layer and output layer. The specific software structure of information sharing security protection system is shown in Figure 1:

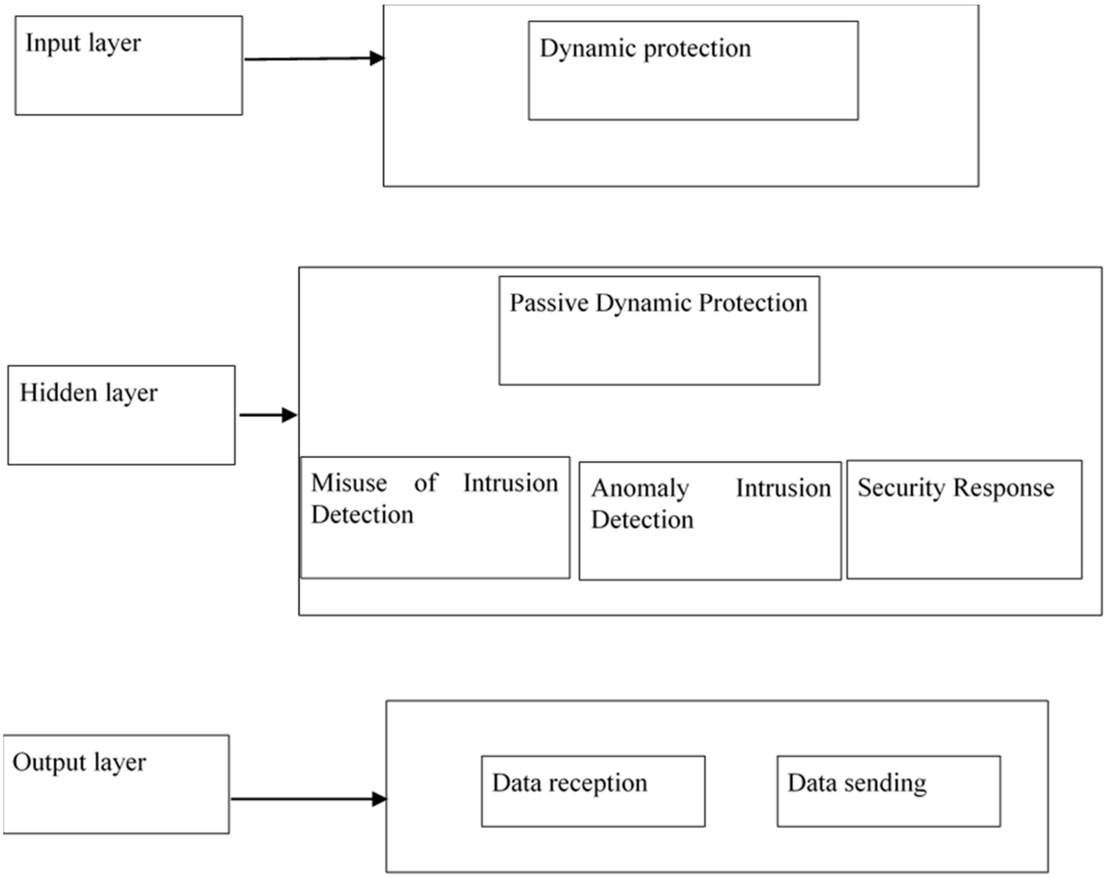

Fig. 1. Software structure of information sharing security protection system

The detailed software functions of the information sharing security protection system based on the recurrent neural network technology in artificial intelligence are as follows:

1) Input layer: The input layer is mainly responsible for information sharing security protection system status information and visual display, mainly for information sharing security dynamic protection.

2) Hidden layer: The hidden layer is mainly the passive dynamic security protection part for information sharing. Passive dynamic firstly performs intrusion detection on the state of the system. On the one hand, the information of the system is analyzed in real time through the recurrent neural network, and the known information attack is detected through feature matching; Predicts the time interval of information communication packets to detect information anomalies. After detecting abnormal information, the security response module generates and issues security response commands to protect the dynamic security of the system.

3) Output layer: The output layer is responsible for data communication with the distributed security switches deployed in the information sharing security site, including network information obtained by mirroring and issuing security instructions generated by the security supervision center.

B. Application of Information Sharing Security Protection System Based on Artificial Intelligence

In order to evaluate the defense effect of the information sharing security protection system, this paper considers two types of information security, namely information misuse (IM), information anomaly (IA) and security response (SR). And selected 50%, 100%, 150% and 200% of the information samples to test the detection and protection accuracy. Firstly, the sum value of Euclidean distances between a single gradient and other gradients in the gradient set is calculated, and then the gradient with the smallest sum value of Euclidean distances is selected as the latest gradient to update the weights of the recurrent neural network model. Specific experimental results are compared as shown in Figure 2:

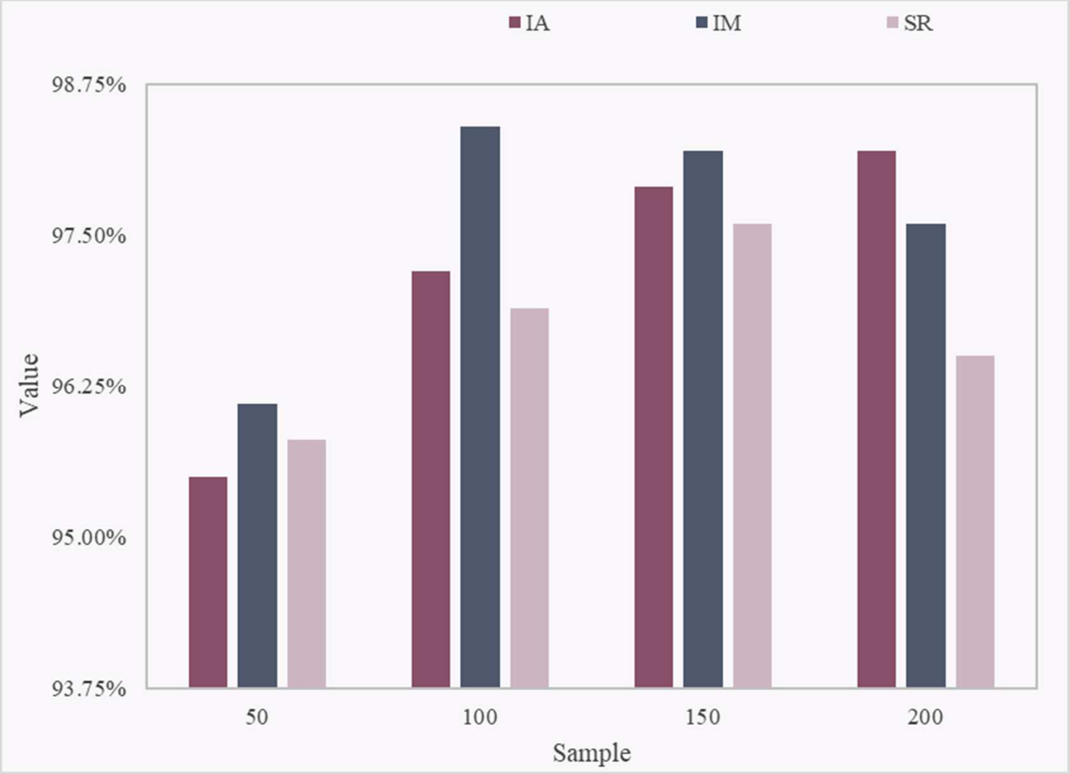

Fig. 2. Comparison of experimental results of protection accuracy

As can be seen from the experimental data in Figure 2, the security defense effect of information sharing based on recurrent neural network is better. In the detection and defense of information misuse (IM) samples from 50% to 200%, the accuracy rate of the information sharing security protection system based on (RNN) reaches 98.4% and 96.1%, respectively. In the detection and defense of 50% to 200% of information anomaly (IA) samples, the accuracy of the information sharing security protection system based on recurrent neural network (RNN) is in the range of 95.5% to 98.2%. In the detection and defense of 50% to 200% of information security response (SR) samples, the accuracy rate of information sharing security protection system (RNN) reaches 95.8% and 97.6% respectively.

V. Conclusion

This paper expounds the information sharing based on artificial intelligence technology to establish safety protection system, neural network contains a loop equation, and the application of artificial intelligence technology in information sharing security and safety description of the elements of information sharing, and information sharing based on the artificial intelligence security protection system design, system environment and the parameter configuration of investigation and study, at the same time The process framework of information sharing security protection system based on artificial intelligence is designed. Through the experimental test, the superiority of the information sharing security protection system based on artificial intelligence is proved.

References

[1] El-Latif A A, Abd-El-Atty B, Venegas-Andraca S E, et al. Efficient quantum-based security protocols for information sharing and data protection in 5G networks. Future generation computer systems, 2019, 100(Nov.):893-906.

[2] Romansky R P, Noninska I S. Challenges of the digital age for privacy and personal data protection. Mathematical Biosciences and Engineering, 2020, 17(5):5288-5303.

[3] Haque S, Kumar K, Haque A, et al. Blockchain Technology for IoT Security. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(No 7):549-554.

[4] Parfenov D I, Bolodurina I P, Torchin V A. Development and Study of Algorithms for the Formation of Rules for Network Security Nodes in the Multi-Cloud Platform. Modeling and Analysis of Information Systems, 2019, 26(1):90-100.

[5] Mohammadi A, Hamidi H. Analysis and Evaluation of Privacy Protection Behavior and Information Disclosure Concerns in Online Social Networks. International Journal of Engineering, Transactions B: Applications, 2018, 31(8):1234-1239.

[6] Tom N, Izabela P, Ian M, et al. Barriers and facilitators to engagement with artificial intelligence (AI)-based chatbots for sexual and reproductive health advice: a qualitative analysis. Sexual Health Sex. Health, 2021, 18(5):385-393.

[7] Idowu S O, Fatokun A A. Artificial Intelligence (AI) to the Rescue: Deploying Machine Learning to Bridge the Biorelevance Gap in Antioxidant Assays:. SLAS Technology, 2021, 26(1):16-25.

[8] Swpu P. Recent progress and new developments of applications of artificial intelligence (AI), knowledge-based systems (KBS), and Machine Learning (ML) in the petroleum industry. Petroleum, 2021, 6(4):319-320.

[9] Kim H W, Lee J S. Results of development and application of convergence talent training (STEAM) programs using Artificial Intelligence (AI) and Big Data. Journal of Korean Society for the Study of Physical Education, 2021, 26(2):37-51.

[10] Mohammad M, Saleh A, Jawabreh O, et al. Artificial Intelligence (AI) And The Impact Of Enhancing The Consistency And Interpretation of Financial Statement in The Classified Hotels in Aqaba, Jordan. Academy of Strategic Management Journal, 2021, 20(S(3)):1-18.

[11] Guha S. Public perspectives on Healthcare and Artificial Intelligence (AI): A survey study. International Journal for Innovation Education and Research, 2021, 9(7):1-8.