Research Article

Yingle Yu*

Big data network security defense mode of deep learning algorithm

https://doi.org/10.1515/comp-2022-0257
received May 11, 2022; accepted September 9, 2022

Abstract: With the rapid development and progress of big data technology, people can already use big data to judge the transmission and distribution of network information and make better decisions in time, but it also faces major network threats such as Trojan horses and viruses. Traditional network security functions generally wait until the network power is turned on to a certain extent before starting, and it is difficult to ensure the security of big data networks. To protect the network security of big data and improve its ability to defend against attacks, this article introduces the deep learning algorithm into the research of big data network security defense mode. The test results show that the introduction of deep learning algorithms into the research of network security model can enhance the security defense capability of the network by 5.12%, proactively detect, and kill cyber attacks that can pose threats. At the same time, the security defense mode will evaluate the network security of big data and analyze potential network security risks in detail, which will prevent risks before they occur and effectively protect the network security in the context of big data.

Keywords: deep learning algorithm, big data, network security, defense mode

1 Introduction

The current network development is very rapid, but there are inevitably some loopholes in its development process. In addition, traditional firewalls, loopholes, scanning software, and other security systems cannot effectively resist network attacks, making it the main target of network attacks. To address these issues, more advanced technologies are rapidly being introduced to improve security capabilities and further improve network security, but few people have introduced deep learning algorithms into network security research. Therefore, it is of great significance to study the behavior of combining deep learning algorithms with big data network security defense models in this article.

In the context of big data, people's lives are closely related to the network, and the security of the network is related to people's survival and development. To improve the ability of network security defense, many people have carried out research on network security. Wang proposed an improvement of translation reliability analysis based on the structural reliability analysis of network security technology [1]. Because traditional hacking techniques and firewall techniques cannot effectively resist virus attacks, Ding et al. proposed an architecture design of an intrusion prevention system that integrates auditing and network defense functions [2]. Zhao and Song believed that we should start from three aspects of strategy, management, and technology, and build a more reliable network security system on the basis of traditional passive defense and active defense technology [3]. Wagner et al. examined network-level defense mitigations and quantified their impact on network security and mission performance [4]. Zhao et al. proposed a new game-based approach to simulate the behavior of an adversary network when attacking a competing defense pattern [5]. Li and Li introduced the common methods and tools for evaluating network security in detail and analyzed the application status of various technologies in network security evaluation [6]. Bienstock and Escobar described a stochastic defense mechanism designed to detect complex mesh attacks involving physical actions and changes in sensor output, which are attack model architecture, attack architecture optimization technology, attack measurement, and scale analysis technology [7]. From this point of view, the research results on network security defense have been very extensive, but few people have introduced deep learning algorithms into the research of big data network security defense models. To better construct the defense mode of big data network security,

* **Corresponding author: Yingle Yu,** Tandon School of Engineering, New York University, Brooklyn 11201, New York, USA, e-mail: yuyingle3318@163.com

this article introduces the deep learning algorithm into the research of defense mode.

Deep learning algorithm is an algorithm technology based on the artificial neural network. In recent years, it is emerging as a powerful machine learning tool, which is expected to reshape the future of artificial intelligence. Hence, many people have conducted research on deep learning algorithms. Since most hyperspectral data classification does not extract deep features hierarchically, Chen et al. introduced the concept of deep learning algorithms into hyperspectral data classification [8]. Oshea and Hoydis presented and discussed several new applications of deep learning algorithms at the physical layer, including communication applications, human–computer interaction applications, and applications in the field of monitoring systems [9]. Ravi et al. conducted a comprehensive up-to-date review of research using deep learning algorithms in health informatics [10]. Tom et al. examined critical learning-related models and methods for multidisciplinary projects and provided their evolution [11]. Zhu et al. analyzed the challenges of using deep learning for remote sensing data analysis and provided resources that we hope to make deep learning in remote sensing seem ridiculously simple [12]. Wang et al. proposed a fingerprint recognition system for indoor localization with calibrated channel state information and phase information [13]. Majumder et al. proposed a deep learning algorithm-based method for determining the author's personality type of text [14]. From this point of view, the research results of deep learning algorithms have been very rich, but the application in network security is lacking.

To better study the big data network security defense mode, this article introduces the deep learning algorithm into the research. The network has played an important role in education, training, employment, and human life style, and it has gradually become a necessity of human life. People's trust in the network is increasing day by day. However, the development of big data network security has increased the technical problems of network security and has also brought frequent pressure and pressure on people's lives. Therefore, the importance of network security has become a hot topic of social debate. To protect the big data network security and improve the network security defense ability, this article studies the big data network security defense mode based on the deep learning algorithm.

2 Big data network security defense mode

2.1 Network security active defense system

The active defense of network security is a concept proposed for the passive defense of traditional security [15]. Traditional network security defense methods usually take actions according to the attack situation after the system is attacked, which has obvious drawbacks. It has obvious drawbacks, and it is easy to cause network paralysis and large economic losses. It is clearly insufficient to face the current complex network environment and various security threats with traditional network security defense methods. To solve the problem that traditional network security defense methods cannot face various current network attacks, this article analyzes the big data network security system based on deep learning algorithms. The network security active defense system is shown in Figure 1.

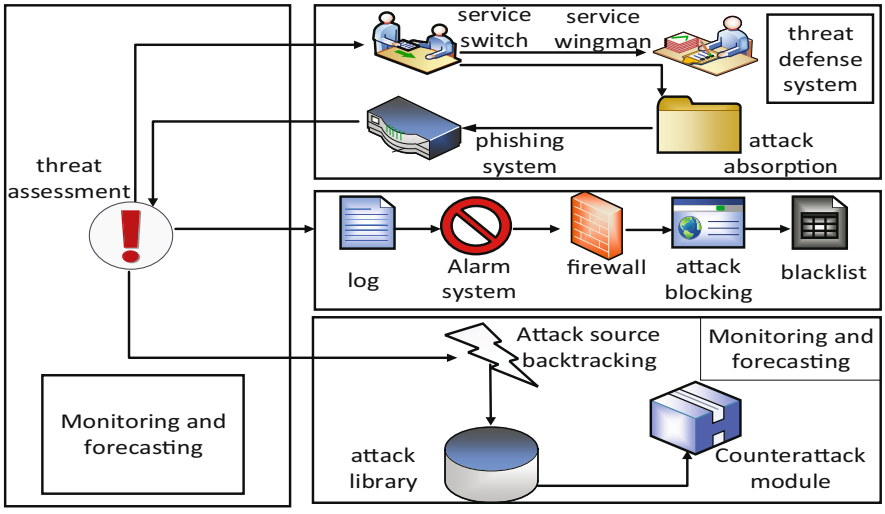

Figure 1: Network security active defense system diagram.

As shown in Figure 1, according to the different operating modes, the active network security system can be divided into two parts: the defense module and the counterattack module. The defense module includes intrusion detection, automatic switching software, and attack recovery module, and the counterattack module includes the attack source grammar and the counterattack module. When the attack occurs, the network security of the intrusion software will correct the attack behavior of the fraudulent system and disconnect the connection with the host illegally. When the server is shut down and cannot provide services normally, the service conversion software will automatically complete the work conversion, and the wingman service will continue to provide services. The counterattack unit detects the speed-based reverse attack, calculates the attack behavior according to the nuclear power rated unit, and selects the performance modification attack of the corresponding density in the counterattack technology. The network trick is activated to serve the security system, and the host wingman software will decide whether to activate the shift module based on the search results. An active network security system will judge the attack behavior from the aspects of hacker attack, hacker's access to the control network, and attack and forwarding attack according to the attack subject, to activate the defense behavior and prevent the network attack.

2.2 Pre-alarm system

The early warning system is the key to the network security defense model to predict unknown risks and actively detect and kill threats [16]. The prealarm system can actively analyze various network attacks existing in the network, actively analyze sound intrusion alarms, indirectly solve the network security threats brought by network attacks, and protect network security. The functional structure of the prealarm subsystem is shown in Figure 2.

As shown in Figure 2, early warning is mainly divided into three parts, namely, early warning center, low-level clustering unit, and intrusion alarm collector. When an unknown network attack is detected, the prealarm analysis module will transmit the monitored data to the high-level security state management module. Then, the module will transmit the information retrieved from the database to the lower-level clustering unit through the communication module. The basic premise of the early warning background system is divided into three levels: intrusion alarm, cluster, high-level regular expression, and custom prediction. Note that the system is suitable for large-scale networks, and compilation and intelligent operations are carried out through network sharing. Network sharing divides the entire network into multiple domains, and each area can have multiple

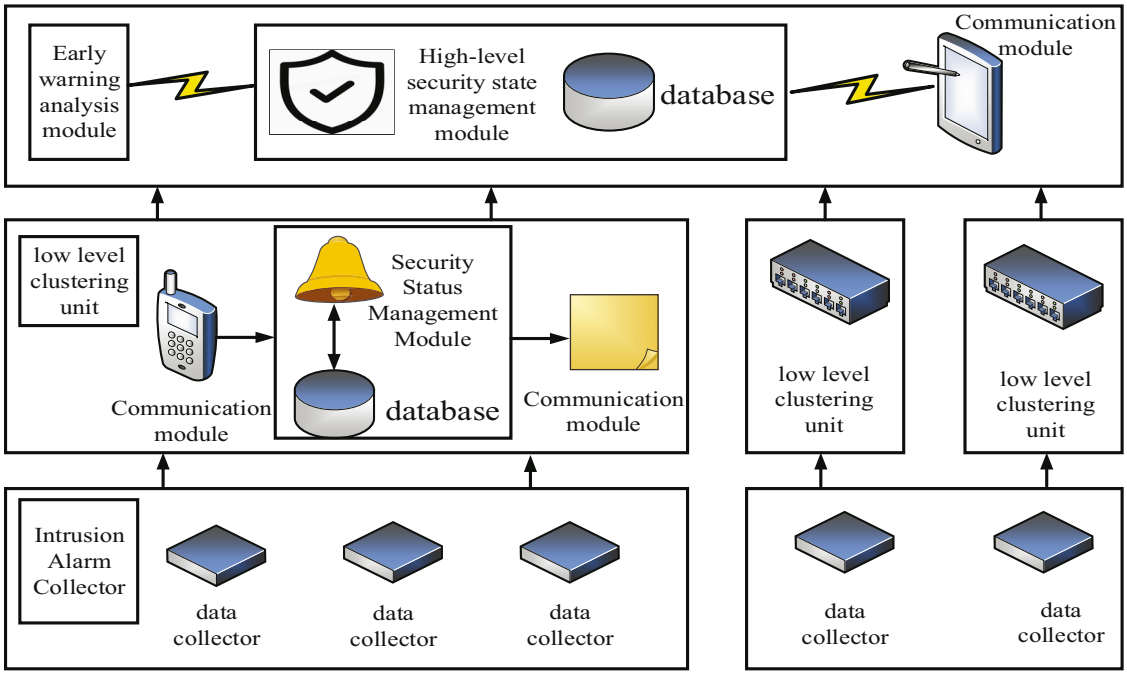

Figure 2: Functional structure diagram of the prealarm subsystem.

network components to facilitate the collection and processing of information. Each network partition represents a low-level cluster unit, and each low-level cluster unit has multiple incoming alert receivers and an alert analysis element. Each network unit carries an infected alert receiver that is responsible for receiving information about unknown cyber attacks. The low-level cluster segment adopts the cluster analysis method for the alarm information and identifies the related attack events and their distribution, and the analysis results are confirmed by the early warning center. The early warning system is an important part of big data network security, which can warn network attacks in advance and protect network security.

2.3 Automatic attack module

Only relying on the prealarm system to defend against network attacks is not a sure-fire way to protect network security fundamentally. To better research the network security defense mode of big data, this article investigates the intrusion rate of attacks on the system according to possible system security vulnerabilities and identifies the automatic attack system. The network attack system integrates the existing security attack technology and uses a variety of attack methods and tools to attack the host area or host service according to the basic network attack process. The automatic attack module is shown in Figure 3.

As shown in Figure 3, the network attack planning steps include: information system detection, data collection, security vulnerability analysis, and information system security attacks. In the automated attack module, the information system search module will record and analyze the network settings of the specified information system by performing specific information system analysis. The host information collection part will summarize the host information and host site operation information according to the security system, analyze the existing security vulnerabilities, identify the vulnerable vulnerabilities in network security, and provide the required vulnerability information for the security attack module. In the security attack unit, power escalation and surveillance cover-up belong to nondestructive attacks, which are used to gain superuser benefits and eliminate relevant control records, respectively, to avoid the detection of attacks. The automatic attack module can always detect and solve the vulnerabilities of the current data network security function during the attack process, effectively protect the network security, and enhance the big data network security capability.

2.4 Network security protection relationship

Cybersecurity is an advanced technology that uses a wide range of security products to achieve general security [17], including physical security and intellectual security.

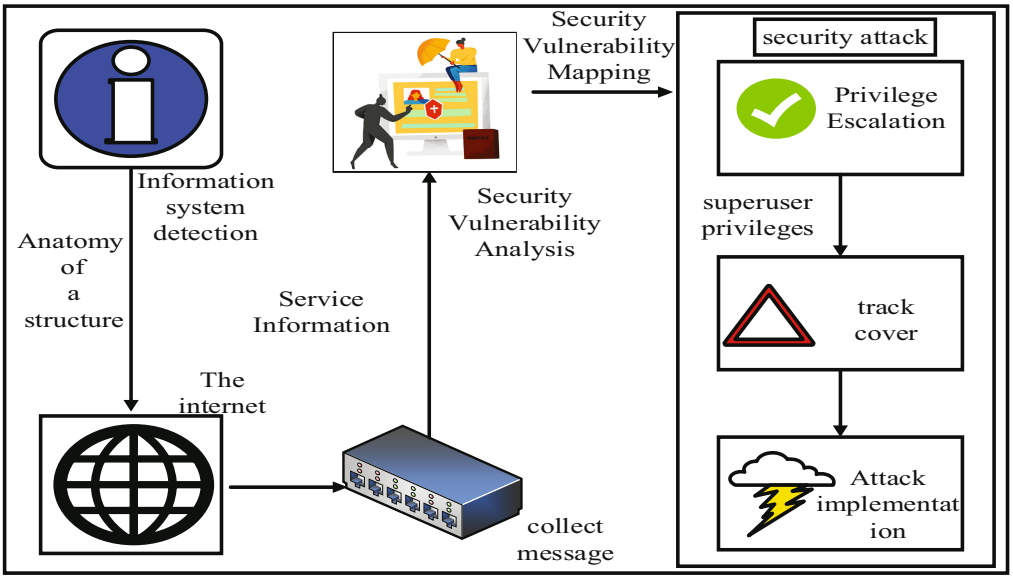

Figure 3: Automatic attack module diagram.

Physical security refers to the electrical and physical security of computer network systems and related applications to prevent damage and loss. Information security refers to the confidentiality, confidentiality, and availability of information in the process of information exchange and transmission. Controlling the security depth relationship of information flow can better understand the security applications and security functions of the system and improve the defense capability of big data network security. The network security protection relationship is shown in Figure 4.

As shown in Figure 4, the network security relationship diagram illustrates the entire security process from source to source from the perspective of information security. The entire information flow process is secure, and each stage has different security requirements. Human–computer interaction security requires authentication, authorization, and access control; LAN security requires workspace security, server security, subnet security, source code control, and internal security, while border security requires network control; general cybersecurity requires confidentiality, integrity, and availability of information transmissions. Understanding the network security protection relationship is one of the important foundations for the research on the big data network security defense model.

2.5 Evaluation model of network security defense system

The combined strength analysis of network security components is the basic work for the research of the network security defense mode [2]. The big data network security defense mode requires that the components have consistent overall security policies, and their network security defense functions can be realized. This article adopts the network security defense system evaluation model, and the specific framework is shown in Figure 5.

As shown in Figure 5, the specific process of the network security defense system is as follows: first determine the research basis of the big data network security defense mode and then investigate the relative position of the components to ensure that the components meet the functional design requirements. Only by determining the order of understanding of data and groups, the trust between data and the efficiency of evaluation results be further improved. The component identification process is the basis of component rating, and the relationship between components is very important for component identification. The analysis of network system components is essential because analyzing the total strength of network system components is the basis for determining the impact of security components on network

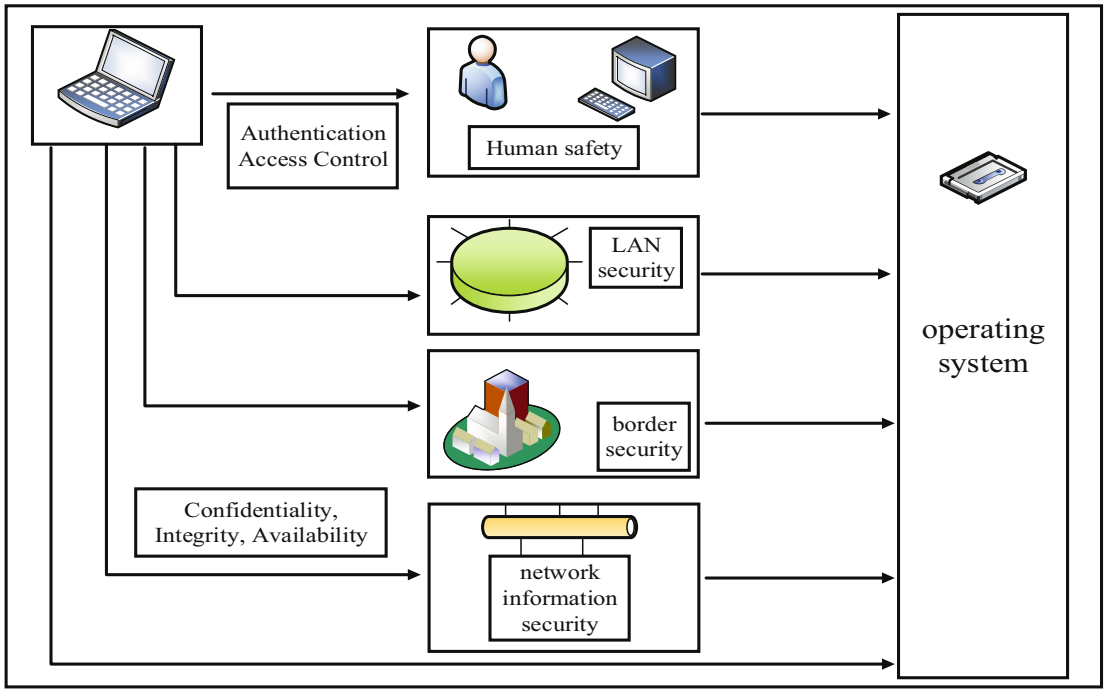

Figure 4: Network security protection relationship diagram.

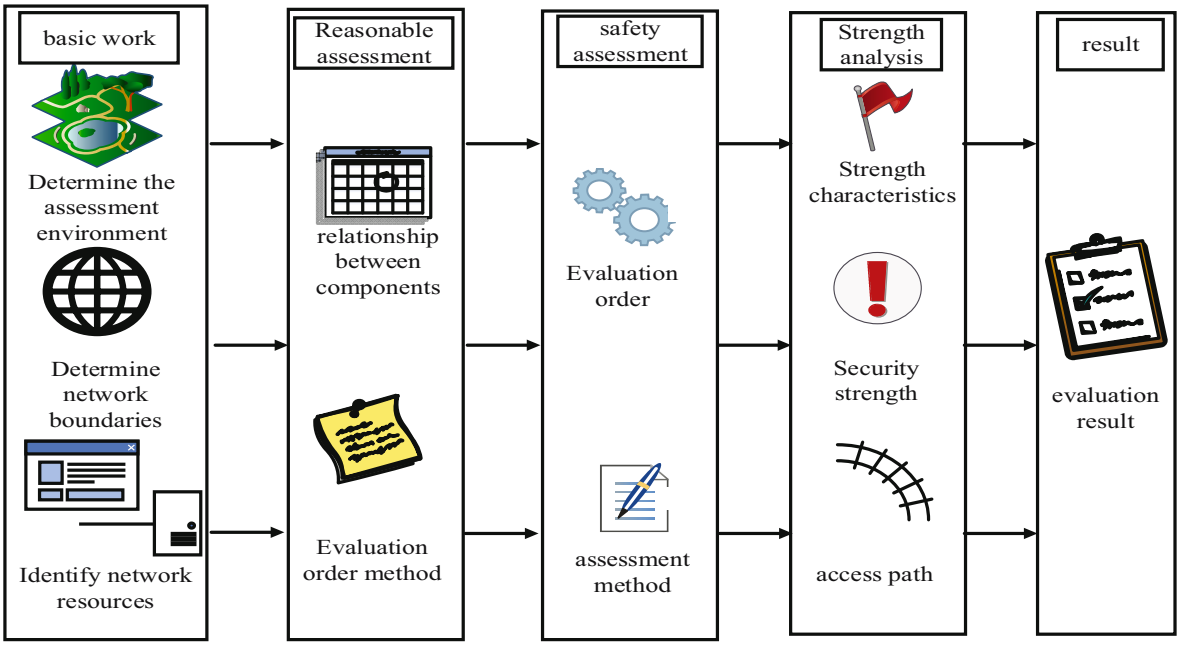

Figure 5: Framework diagram of network security defense system evaluation model.

security. If the network security analysis only focuses on the entire network, it is impossible to distinguish the security components and security sources in the network system. Therefore, the network security should be ensured by analyzing the relationship between the characteristics of the components and the access routes.

Among them, x_j represents the input vector of the first neuron. w_{ij} represents the neuron density and the number of j; θ_j represents the threshold of neuron j; and Y_j is the output value of neuron j. When Nj activates neurons beyond the limit, it has a surprising effect on the network. When the neuron activation level is less than or equal to the threshold, there is an inhibitory effect on the network.

3 Deep learning algorithms

3.1 Neuron output

A neuron has two states [18]: an activated state or an inhibitory state, denoted by positive 1 and negative 1, respectively. The expression for the neuron is expressed as follows:

$$y_j = s\left(\sum_{i=1}^{n} w_{ij}x_i - \theta_j\right), \tag{1}$$

where θ_j is the jth functional neuron, and s is expressed as follows:

$$y_j\begin{cases} + \sum_{i=1}^{n} w_{ij}x_i > \theta_j \\ - \sum_{i=1}^{n} w_{ij}x_j \le \theta_j. \end{cases} \tag{2}$$

3.2 Classical learning algorithm

A commonly used unipolar function is chosen as the function to activate neurons [19].

$$f(u) = 1 + e^{1}_{-u}, \tag{3}$$

and its derivative is expressed as follows:

$$f'(u) = f(u)(1 - f(u)). \tag{4}$$

Activation function for each node is expressed as follows:

$$a_j^l = f\left(\sum_{i=0}^{N_{l-1}} w_j^l, a_i^{l-1}\right). \tag{5}$$

Among them, a_j^l represents the activation value of the jth node of the lth layer through the transfer function, and the density factor between the ith unit of the lth layer and the jth unit of the lth layer is w_j^i.

3.3 Network objective function

The network objective function, or network loss function, is the performance function of the network, and one of the two parameters is necessary to compile a model.

$$Jp(t) = \frac{1}{2}\sum_{R} dRp - yRp^2. \tag{6}$$

Among them, $J_{Rp}(t)$ is the objective function when the pth group is input [20].

3.4 Convolutional layer gradient

In the convergence layer, by performing the motion function on the convergence kernel and the input layer of this layer, it is possible to choose whether to perform random operations and development functions in the new version and finally obtain the conjunctive function of the next layer. Its calculation process is expressed as follows:

$$x_j^l = f\left(\sum_{i\in M_j} x_j^{l-1} \star k_{ij}^l + b_j^l\right). \tag{7}$$

3.5 Gradient of residual map

$$\delta_j^l = \beta_j^{l+1}(f'(u_j^l) \star \mathrm{up}(\delta_j^{l+1})), \tag{8}$$

where $J_{Rp}(t)$ represents a sampling operation.

3.6 Pixel copy operation

$$\frac{\partial E}{\partial k_{ij}^l} = \sum_{u,v} (\delta_i^l)_{uv} (P_{ij}^{l-1})_{uv}. \tag{9}$$

3.7 Downsampling layer gradient

The downsampling layer gradient propagates the remaining layers forward through the layer-by-layer gradient from the back layer to the front layer, while multiplying the densities between different layers. The calculation formula is:

$$\delta_j^l = f'(u_j^l) \star \partial k_{ij}^{l\partial J}. \tag{10}$$

3.8 The calculation formula of the input layer

$$f_j^l = \sigma\left(\sum_{i\in M_j} f_i^{l-1} \star w_{ij}^l + b_j^l\right). \tag{11}$$

Among them, f_j^l represents the mapping of the jth part of the lth layer, M_j is the development function of the neuron and represents the number of tensors corresponding to the hidden layer array, $*$ represents the convergence, w_{ij}^l represents the jth convolution kernel of the lth layer, and b_j^l represents the bias term.

3.9 Pooling layer calculation formula

$$f_j^l = \sigma(\beta_j^l d(x_j^{l-1}) + b_j^l), \tag{12}$$

where $d()1$ represents a reduction function applied to random regions in the image.

3.10 Decision loss function

The decision loss function is the sum of the weights of the position loss and the confidence loss, and its expression function is expressed as follows:

$$L(x) = \frac{1}{N}(L_{\mathrm{conf}}(x, c) + \alpha L_{\mathrm{loc}}(x)). \tag{13}$$

Among them, N is the default number of frames; $L_{\mathrm{loc}}(x)$ is the position loss, that is, the amount of loss between the predicted frame and the ground truth frame; $L_{\mathrm{conf}}(x)$ is the information loss; $\alpha = 1$; and $L_{\mathrm{loc}}(x)$ shows the prediction loss.

3.11 Prediction loss function

$$L_{\mathrm{loc}}(x) = \frac{1}{2}\sum_{i,j} x_{ij}^p ||l_i - g_j^p||^2. \tag{14}$$

3.12 Activation function

$$f_s(x) = \frac{1}{1 + e^{-x}}, \tag{15}$$

$$\lim_{x\to\infty} f_s'(x) = 0. \tag{16}$$

3.13 Gradient vanishing function

$$f_t(x) = \frac{1 - e^{-2x}}{1 + e^{-2x}}. \tag{17}$$

3.14 Momentum term function

$$x_{t+1} = \beta \Delta x_{t-1} - \ \lg. \tag{18}$$

Among them, β is the momentum coefficient, and $\beta \in [0, 1]$ indicates how much this gradient update retains the gradient direction of the previous update.

3.15 Sample training set

$$C = \frac{1}{m}\sum_{i=1}^{m}(\Phi^i). \tag{19}$$

3.16 Gradient loss function

$$\frac{\partial C}{\partial b^{k+1}} = \frac{1}{m}\mathrm{sum}^r(\zeta^{k+1}). \tag{20}$$

Among them, the obtained gradient loss value is scaled according to a certain proportion, and the adjustment amount of each layer parameter can be obtained.

4 Method of big data network security defense mode

Big data is a very advanced process identification method, which can find hidden, valuable data sources from big data that can help people make important decisions. Currently, big data has been widely used in literature retrieval, interdisciplinary, weapon management, and other fields, and is at the advanced level of social intelligence. Many viruses or trojans use more advanced attack methods that can save longer time and infect a wide range of networks, causing more serious economic losses. Therefore, this article uses big data technology and deep learning algorithms to study the network security defense patterns together with other modes. To facilitate the research, this article names different defense modes as mode 1, mode 2, mode 3, mode 4, and mode 5, where mode 5 is the big data network security defense mode studied in this article. To better understand the big data network security defense patterns studied in this article, the ability of different defense modes will be analyzed by the scoring system of 0–10 points.

5 Results of big data network security defense mode

5.1 Processing capability of different defense modes on the same attack

The ability to process cyber attacks is the main content of network security defense mode research because the defense mode is to handle network attacks. To further understand the processing ability of the network security defense patterns on the same network attack based on deep learning, this article studies the different defense modes together. The specific research data are shown in Figure 6.

As shown in Figure 6, the five network security defense modes are all equipped with attack prediction, forecast, police, vulnerability patch, active investigation, and killing. In terms of attack prediction ability, the attack prediction ability of modes 1–4 is far less than that of the network security mode studied in this article, and it is difficult to discover unknown network attacks in time and protect the network security. In terms of forecast warning and active detection capability, the capability of modes 1–3 is clearly lower than the network security defense mode studied in this article, while the capability of mode 4 is higher than mode 5, indicating that there is still a lack of the defense mode, which is studied in this article, which needs to be constantly studied to promote the development of network security defense mode. On the whole, the ability of the network security defense mode to the same attack is relatively high, but there is still room for improvement.

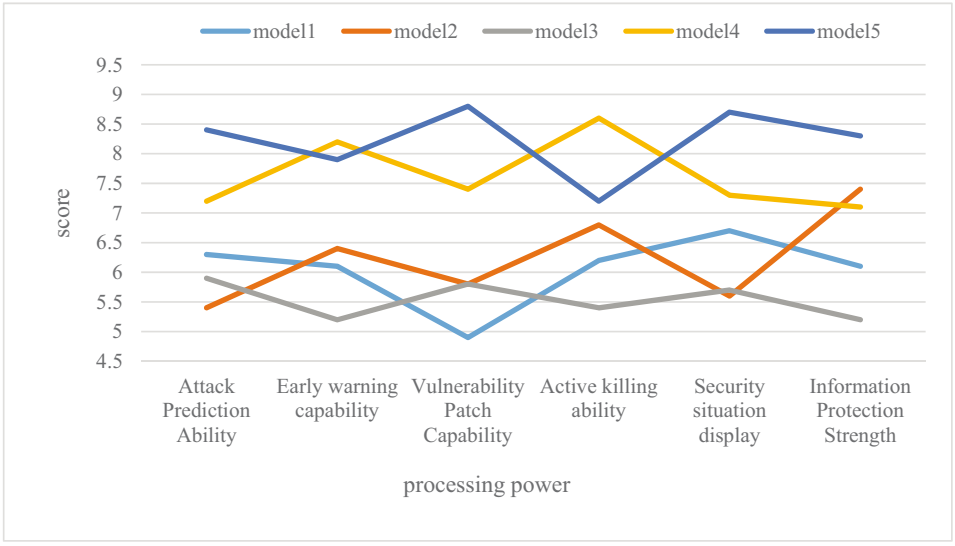

Figure 6: The processing capability of different defense modes to the same attack.

5.2 The capability of different defense modes to handle different network attacks

The network security defense mode helps to study the processing ability of network attacks to protect network security. To more clearly demonstrate the ability of defense patterns to process different network attacks, this article studies different network security defenses together with the defense modes studied based on deep learning. The specific data are shown in Figure 7.

As shown in Figure 7, different network security defense modes have different processing modes for different network function attacks. Mode 2 has the lowest processing power when handling computer vulnerabilities, and the network security defense mode presented here has the highest processing power compared to the other four modes. In dealing with network fraud, mode 1 has the weakest processing power, while mode 3 has a strong processing power, at around 6.5 points. When dealing with computer vulnerabilities, mode 3 has the weakest processing capacity compared to the other four modes, with only about 4 points, which is far less than the network defense mode studied in this article. When handling hackers, mode 4 is relatively powerful, far less than other defense modes. In general, modes 1 to 4 are not good at dealing with network attacks, and it is difficult to fully guarantee the security of the network. For the network security defense methods studied in this paper, a mode with strong network defense attack capability should be selected to ensure network security and maintain network order to a large extent.

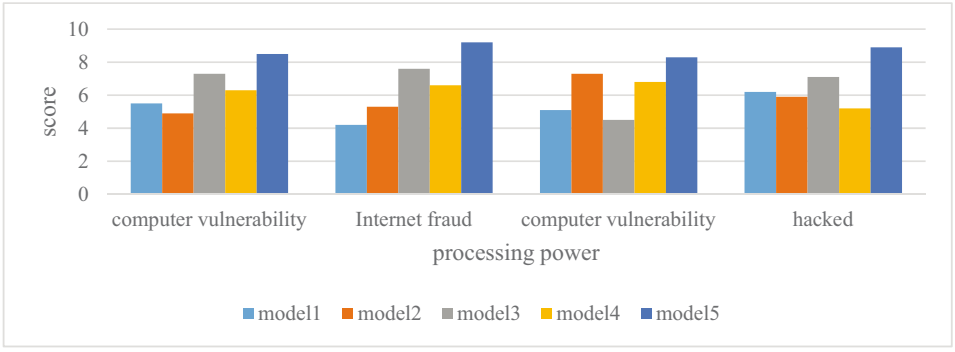

Figure 7: The ability of different defense modes to deal with network attacks.

5.3 Information and data security of different defense modes

To protect the network, the information data of the network is protected because the information data on the network is related to everyone's privacy and life. To select a better network security defense mode to protect the security of information data, this article studies the information data security of different defense modes. The specific data are shown in Figure 8.

As shown in Figure 8, the security of information data mainly includes six aspects: information collection, storage, transmission, application, sharing, and destruction. On the whole, mode 2 has the worst protection ability in information data security, while modes 1 and 4 are medium to protect information data security, but still far from the protection capability of modes 3 and 5 in information data security. From the data point of view, mode 3 has a score of 7 points in protecting the security of information and data, and the degree of protection of information and data is very high. The network security mode studied in this paper, namely mode 5, has a score of 8 points in protecting information and data security, which is higher than that of mode 3, which shows that the network security defense mode proposed in this paper can protect information security to a greater extent.

5.4 Defense capability of different defense modes

The ability to defend against network attacks is the basis of the network security defense mode. Only when the defense mode of network attacks is improved, can we better protect the network security under the background of big data. To test the defense capability of the network security defense mode, the no-use defense mode is studied together, and the specific research data are shown in Figure 9.

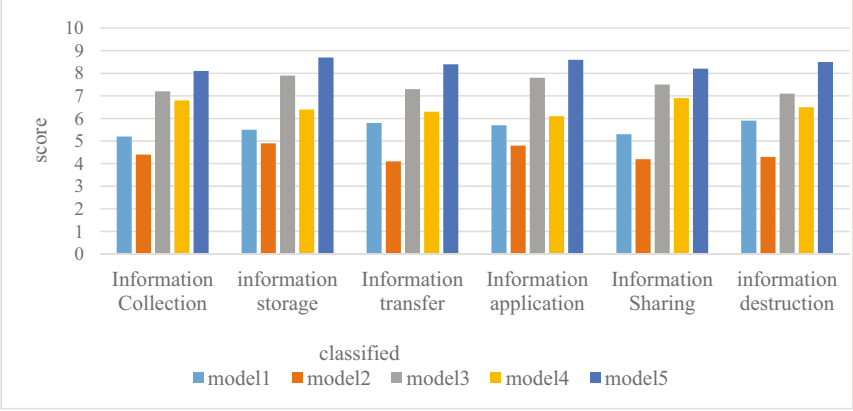

Figure 8: Information and data security of different defense modes.

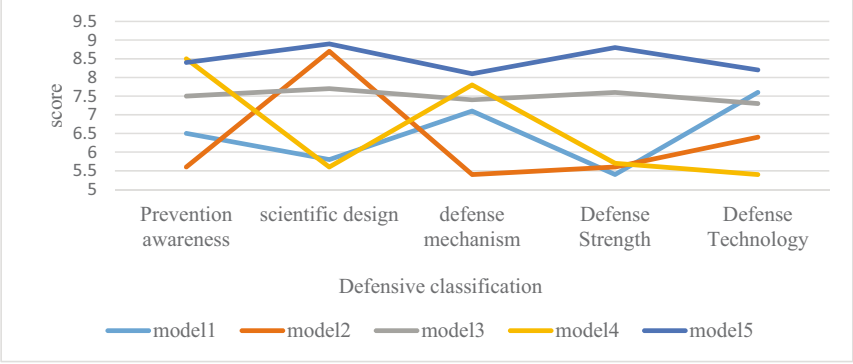

Figure 9: Defense capabilities of different defense modes.

As shown in Figure 9, mode 1 has the lowest capability in terms of scientific design and defense strength, but it is relatively high in terms of defense mechanisms and defense technology, which can protect network security to some extent. Mode 2 is not only relatively weak in defense mechanism but also strong in scientific design. In other aspects, it is difficult to protect the security of the network. Mode 3 has a relatively balanced defense capability in all aspects, mostly around 7.5 points, which can protect network security to a large extent. Mode 4 has a strong ability in terms of defense mechanism, the worst ability is in terms of scientific design and defense technology, only about 5.5 points, and the overall defense ability is relatively good. Compared with the other four defense modes, the defense capability of mode 5 is relatively strong, and it is relatively balanced to protect the security of the network from all aspects. That is to say, the defense ability of the big data network security defense mode is relatively strong, which is the best choice to protect the network security.

5.5 Defense efficiency of different defense modes

If the defense mode is only aimed at network security, and the defense capability is not strengthened, its defense effect cannot be guaranteed. To conduct in-depth study of big data network security defense mode, this article introduces the defense efficiency into the study of network security defense mode-specific research data as shown in Figure 10.

As shown in Figure 10, to study the defense efficiency of network security mode, we need to study from six aspects: attack blocking, monitoring perception, attack analysis, attack absorption, security, and information leakage. Mode 1 is more efficient, but only about four points in attack analysis, which is less efficient. Mode 2 is less efficient in security than others. Mode 3 scored above 6 points in each defense aspect, and the overall defense efficiency is relatively high. Mode 4 has the highest score in information leakage and a relatively low score in other aspects, indicating that mode 4 cannot fundamentally guarantee the security of the network. In terms of attack blocking, monitoring perception, and attack absorption, the score of mode 3 is relatively high, mostly around 7 points, indicating that the defense efficiency of mode 3 is acceptable to a certain extent. Compared with the other four defense modes, mode 5 has a relatively high defense efficiency, because mode 5 has a relatively high score in all aspects, which can well protect the network security.

6 Conclusion

Today, big data technology has been widely used in many fields, with strong integration and permeability, so the role and operation of big data technology has been effectively integrated into the return. However, big data technology also has many characteristics, such as openness, and we need to consider the network security prevention work and take effective measures to optimize and improve it. To protect the network security and improve the network security defense capability, this article studies the big data network security mode based on the deep learning algorithm, aiming to provide a reference for promoting the defense mode of computer network security.

(1) Different defense modes are very different in the processing capacity of the same attack. The five network

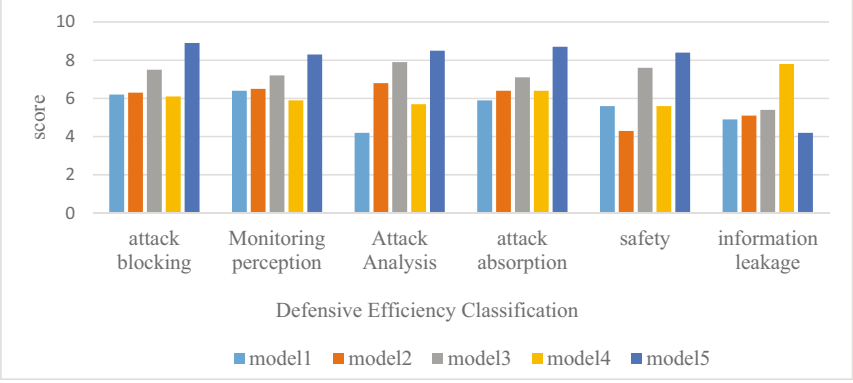

Figure 10: Defense efficiency of different defense modes.

security defense modes are all equipped with attack prediction, forecast, police, vulnerability patch, active search and killing, security situation display, and information protection capabilities, but they are different in different capabilities. Mode 1-mode 4 is far less capable of handling the same network attack than the network security model studied in this paper, and it is difficult to detect unknown network attacks in time and protect network security. However, on the whole, the network security defense model still needs to be improved.

(2) Different defense modes have different processing capabilities to different network attacks. Different network security defense modes have different processing modes for different network function attacks. In processing different network attacks, the processing capacity of the network security defense mode studied is the highest compared with the other four modes, which can guarantee network security and maintain network order to a large extent.

(3) The information and data security of different defense modes is different. On the whole, the information and data security of the network security mode studied in this article is relatively high, which shows that the big data network security defense mode studied based on the deep learning algorithm can protect the information security to a large extent.

(4) The defense capabilities of different defense modes are determined by differences. The defense capability of the network defense mode is mainly divided into four aspects: prevention, consciousness, scientific design, defense mechanism, defense strength, and defense technology. Compared with the other four defense modes, mode 5 has a relatively strong defense ability and a better balance that can be protected from all aspects.

Conflict of interest: The author declares that there is no conflict of interest with any financial organizations regarding the material reported in this manuscript.

Data availability statement: Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] S. Wang, "Attack mode and defense mechanism based on computer network security," *IPPTA: Q. J. Indian. Pulp Pap. Technical Assoc.*, vol. 30, no. 6, pp. 354–359, 2018.

[2] S. Ding, Z. Zhang, and J. Xie, "Network security defense model based on firewall and IPS," *J. Intell. Fuzzy Syst.*, vol. 39, no. 12, pp. 1–9, 2020.

[3] G. Zhao and J. Song, "Network security model based on active defense and passive defense hybrid strategy," *J. Intell. Fuzzy Syst.*, vol. 39, no. 4, pp. 1–9, 2020.

[4] N. Wagner, C. S. Sahin, and M. Winterrose, "Quantifying the mission impact of network-level cyber defensive mitigations," *J. Def. Model. Simul.*, vol. 14, no. 3, pp. 201–216, 2017.

[5] J. Zhao, X. Zhang, and F. Di, "Exploring the optimum proactive defense strategy for the power systems from an attack perspective," *Secur. Commun. Netw.*, vol. 2021, no. 6, pp. 1–14, 2021.

[6] Y. Li and X. Li, "Research on multi-target network security assessment with attack graph expert system model," *Sci. Program.*, vol. 2021, no. 3, pp. 1–11, 2021.

[7] D. Bienstock and M. Escobar, "Stochastic defense against complex grid attacks," *IEEE Trans. Control. Netw. Syst.*, vol. 7, no. 2, pp. 842–854, 2020.

[8] Y. Chen, Z. Lin, and Z. Xing, "Deep learning-based classification of hyperspectral data," *IEEE J. Sel. Top. Appl. Earth Obs. Remote. Sens.*, vol. 7, no. 6, pp. 2094–2107, 2017.

[9] T.Oshea and J.Hoydis, "An introduction to deep learning for the physical layer," *IEEE Trans. Cognit. Commun. Netw.*, vol. 3, no. 4, pp. 563–575, 2017.

[10] D. Ravi, C. Wong, and F. Deligianni, "Deep learning for health informatics," *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 4–21, 2017.

[11] Y. Tom, H. Devamanyu, and P. Soujanya, "Recent trends in deep learning based natural language processing [Review Article]," *IEEE Comput. Intell. Mag.*, vol. 13, no. 3, pp. 55–75, 2018.

[12] X. X. Zhu, D. Tuia, and L. Mou, "Deep learning in remote sensing: A comprehensive review and list of resources," *IEEE Geosci. & Remote. Sens. Mag.*, vol. 5, no. 4, pp. 8–36, 2018.

[13] X. Wang, L. Gao, and S. Mao, "CSI phase fingerprinting for indoor localization with a deep learning approach," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1113–1123, 2017.

[14] N. Majumder, S. Poria, and A. Gelbukh, "Deep learning-based document modeling for personality detection from text," *IEEE Intell. Syst.*, vol. 32, no. 2, pp. 74–79, 2017.

[15] D. Zhang and Q. He, "Security situation awareness method for smart grid," *Int. Core J. Eng.*, vol. 6, no. 5, pp. 49–55, 2020.

[16] M. Matovic, M. Ravlic, M. Jeremic, S. Jankovic, and M. Vlajkovic, "Alarm system for surveillance of patients receiving high doses of radioiodine (~(131)I) therapy in the case of unauthorised abandoning of a controlled area," *Nucl. Technol. & Radiat. Prot.*, vol. 33, no. 2, pp. 223–229, 2018.

[17] X. Zhang, J. Lu, and D. Li, "Confidential information protection method of commercial information physical system based on edge computing," *Neural Comput. Appl.*, vol. 33, no. 4, pp. 1–11, 2021.

[18] A. Vidybida, "Output stream of leaky integrate-and-fire neuron without diffusion approximation," *J. Stat. Phys.*, vol. 166, no. 2, pp. 267–281, 2017.

[19] J. Li, F. Ding, and T. Hayat, "A novel nonlinear optimization method for fitting a noisy Gaussian activation function," *Int. J. Adapt. Control. Signal. Process*, vol. 36, no. 3, pp. 690–707, 2022.

[20] R. Esfandiari, R. Noorossana, and Y. E. Teimour, "An integrated time, cost, and reliability optimization for supply chain design," *Int. J. Oper. Quant. Manag.*, vol. 25, no. 2, pp. 75–90, 2019.