Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 261 (2025) 1050–1056

Procedia Computer Science

www.elsevier.com/locate/procedia

The 5th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT2024)

Architecture design of computer network database protection system based on artificial intelligence

Shengqian Tu*

Faculty of Engineering, Anhui Sanlian University, Hefei 230000, China

Abstract

The purpose of this study is to explore the computer network database protection system based on artificial intelligence, and improve the security protection ability of database by introducing artificial intelligence technology. The system combines advanced machine learning algorithms and deep learning models to monitor database status in real time, identify potential security threats, and automatically take appropriate defensive measures. The experimental results show that the system has remarkable advantages in improving the efficiency of database security protection, reducing the false positive rate and false negative rate, and provides a new solution for the security protection of computer network database.

© 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of The 5th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT2024)

Keywords: Database protection system, Artificial intelligence, Computer network, DDoS attacks;

1. Introduction

In the digital age, computer network database as the core of information storage and management, carries massive privacy data, which is crucial to the normal operation and development of an organization. However, with the popularization of network technology and the increasing complexity of network environment, databases are faced with multiple security threats from external and internal sources, such as hacker attacks, malware intrusion, data leakage and illegal access. These security incidents will not only lead to data loss, damage and disclosure, but also may bring huge economic losses and reputation damage to enterprises and individuals. It is particularly urgent to strengthen the security protection of computer network database. The purpose of this study is to build an efficient

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000 .
E-mail address: 13856925903@139.com

1877-0509 © 2025 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer review under the responsibility of the scientific committee of The 5th International Conference on Machine Learning and Big Data Analytics for IoT Security and Privacy (SPIoT2024)
10.1016/j.procs.2025.04.684

and intelligent computer network database protection system by utilizing the powerful advantages of artificial intelligence technology, so as to improve the ability of database to resist various security threats and promote the stable operation of computer network database.

2. Literature review

2.1. Traditional database protection technology

Access control is the basis of database security. By setting user rights, different users can restrict the access levels of database objects, such as tables, views, and stored procedures. Common access control models include autonomous access control (DAC), mandatory access control (MAC), and role-based access control (RBAC). DAC allows users to decide their own data access rights, which is flexible, but relatively low security. MAC controls the access of subject and object based on the preset security label of the system, which has high security but lacks flexibility. RBAC allocates permissions based on the user's role in the organization, simplifying permission management and improving security and flexibility [1]. However, the traditional access control technology is difficult to cope with the complex and changing network environment and the increasing user rights management needs.

Data encryption is an important means to protect data confidentiality. It converts plaintext data into ciphertext so that unauthorized users cannot read the data content. Common encryption algorithms include symmetric encryption algorithms (such as AES, DES) and asymmetric encryption algorithms (such as RSA) [2]. Symmetric encryption algorithm is fast in encryption and decryption, but complex in key management. Asymmetric encryption algorithm is convenient for key management, but slow for encryption and decryption. In practical applications, symmetric encryption and asymmetric encryption algorithms are usually combined to give full play to the advantages of both [3]. Although data encryption technology protects the confidentiality of data to a certain extent, it is still insufficient to protect the integrity and availability of data after encryption.

Intrusion detection system (IDS) and intrusion prevention system (IPS) are important defenses to protect databases from external attacks. IDS monitors network traffic and system logs and analyzes abnormal behaviors and attack characteristics to discover potential intrusion behaviors. On the basis of IDS, IPS can not only detect intrusion behaviors, but also take measures to block them, such as discarding malicious packets and closing connections. Traditional IDS/IPS is mainly based on rule matching and feature detection technology, which has a good detection effect on known types of attacks, but it is prone to missing and false positives for new and unknown attacks.

2.2. Application status of artificial intelligence in database protection

Machine learning algorithm can automatically learn the normal behavior pattern and attack characteristics from a large number of network traffic data and system logs, so as to realize the detection of intrusion behavior. Common machine learning algorithms applied to intrusion detection include support vector machines (SVM), decision trees, naive Bayes, neural networks, etc. For example, SVM is used to classify network traffic data to distinguish normal traffic from attack traffic. The intrusion detection model is constructed by using neural network, which can recognize various complex attack behaviors by training a large number of sample data. Intrusion detection is a key part of network security protection, aiming to identify malicious activities and unauthorized access in the network [4]. Machine learning algorithms can independently learn normal behavior patterns and attack characteristics from massive network traffic data and system logs to achieve accurate detection of intrusion behaviors. Among many machine learning algorithms applied to intrusion detection, support vector machine (SVM) has attracted much attention. SVM is a supervised learning model whose core principle is to find an optimal classification hyperplane in a high-dimensional space to separate different categories of data points. In the network traffic analysis scenario, SVM builds a classification model by learning a large number of labeled normal traffic and attack traffic data [5]. When new network traffic data is input, the model can accurately determine whether the traffic belongs to normal traffic or attack traffic according to the learned characteristics, so as to realize effective detection of network intrusion [6]. The application of machine learning in intrusion detection has effectively improved the accuracy and efficiency of detection, and can cope with some new attacks.

Artificial intelligence technology also has some new explorations in data encryption and integrity protection, such as using generative adversarial network (GAN) to generate encryption keys and improve the security and

randomness of keys through adversarial training; The integrity verification of data is realized based on blockchain and artificial intelligence technology, and the distributed ledger and immutable characteristics of blockchain are utilized, combined with the data analysis capabilities of artificial intelligence, to ensure the integrity of data during storage and transmission [7]. These emerging artificial intelligence applications provide new ideas and methods for data encryption and integrity protection, and have great development potential. However, at present, these technologies are still in the research and development stage, and there are still some problems and challenges, such as the security and stability of GAN-based key generation technology in practical applications need to be further verified; The technology combined with blockchain and artificial intelligence still needs to be further optimized in terms of performance and scalability.

3. Research method

3.1. Architecture design of protection system based on artificial intelligence

In today's digital age, computer network security is of Paramount importance. The computer network database protection system architecture based on artificial intelligence technology is mainly composed of the following three key levels, as shown in Table 1.

As the underlying support of the entire system, the network base layer consists of various physical network devices, such as switches and routers. This layer uses virtualization technology to process hardware data resources, enabling multiple VMS to share computing, storage, and network resources of the same physical device to achieve dynamic resource allocation and load balancing. The network base layer also implements real-time monitoring of each node of the network system, and once an abnormal node occurs, the system will automatically detect and solve it immediately.

The middle layer of the network plays a key role in the security defense system, which is mainly responsible for the management of data inflow and outflow and the allocation of network resources. It provides technical guarantee for the efficient and safe transmission of network information, and optimizes the distribution mode of information resources to ensure the smooth and stable operation of the network.

The network application layer mainly realizes the user interface and security management function of the system, and may also become the breakthrough of network virus intrusion. To effectively reduce network security risks, technical personnel need to strengthen the protection measures at the application layer, especially the collection and management of log data, so as to ensure the security of user operations. By recording and analyzing user operations, you can discover potential security threats in time and take appropriate measures to ensure the secure and stable running of the network application layer. These three levels work closely together to build a solid network security defense line.

Table 1. Architecture of computer network database protection system based on artificial intelligence

Functional layer	Functional service
Network base layer	Basic hardware facility
Network intermediate layer	Data inflow, data outflow, and network resource allocation
Network application layer	User registration, user login, user access

3.2. Function design of protection system based on artificial intelligence

In the network security protection system, each functional module works together to ensure the stability and security of the network. Data acquisition and preprocessing module is the starting point of network security protection. With various advanced data acquisition tools and a variety of technical means, the module can collect massive raw data in real time and accurately from all nodes of the network, including various devices and running applications. Then, the system carries out preliminary processing of these raw data, which lays the foundation for further analysis.

After acquiring the original data, the data cleaning module carries out in-depth processing on the data, removes irrelevant data, carefully corrects the wrong data, and converts the chaotic original data into high-quality data with

standardized format, accurate content and suitable for subsequent analysis [8].

The anomaly detection module relies on powerful artificial intelligence technology to conduct in-depth analysis of the cleaned data and accurately detect potential abnormal behaviors or security threats mainly by intelligent algorithms. Once an anomaly is found, the detection strategy will be promptly adjusted according to the actual situation to ensure the accuracy and efficiency of the detection.

The Threat Response and Defense module is the last line of defense for network security. When the system detects a potential security threat, the module automatically activates the defense mechanism immediately and takes quick measures to prevent the further spread of the threat. At the same time, the first time to send an alert notification to the system administrator. After receiving an alarm, the administrator can quickly determine the severity of the security event and take appropriate measures to effectively reduce network security risks and ensure the normal operation of the network system.

3.3. Computer network security defense algorithm

First, the system will comprehensively use network monitoring tools, log collection system and other diversified means to collect various types of data in the network environment in a wide and detailed manner. These data involve a wide range of information, from the specific information of the network package to the user's interaction behavior in the network, etc., which provides a solid data foundation for subsequent analysis. In the process of data analysis, the system will specifically mark the abnormal behaviors that have been recognized, so that the subsequent processing and research can be more targeted. However, due to the unavoidable noise and redundant information in the collected original data, these interference factors will affect the quality of the data and the accuracy of the analysis, so it must be pre-processed.

One of the key steps in preprocessing is to extract meaningful features from the raw data. In this paper, it is assumed that there is a specific feature extraction function. This function has a strong conversion ability, which can carry out in-depth analysis and processing of the original data and convert it into feature vectors. The specific conversion relationship is shown in equation (1) [9]. Through such transformation, the data can be more concise and effective, and the key information can be highlighted, which provides convenience for further analysis and judgment based on these characteristics.

$$v = f(\mathrm{x}) \tag{1}$$

In the construction of security defense model, it is very important to extract data features and train the model, such as packet size and transmission frequency. The packet size is measured in bytes, and the transmission frequency is calculated by the number of packets per unit time.

After the completion of data processing, the system enters the model training stage. The system first uses the prepared labeled data set to train the random forest model. The data set can provide rich samples for model learning and help the model accurately identify various patterns. Assuming that the data set in this paper is presented in formula (2), its structure and content will directly affect the training effect and final performance of the model [10].

$$D = \{(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)\} \tag{2}$$

In the given expression, x_i represents the eigenvector corresponding to the i th sample. y_i is the corresponding label, and its value has a specific meaning. When y_i is 0, it means that the sample is in normal state. When the value of y_i is 1, it indicates that there is an anomaly in the sample.

As an integrated model, random forest model is composed of many decision trees. When constructing each decision tree, the feature subset is randomly selected, and the training work is carried out based on the training sample subset obtained by random sampling. In order to achieve better performance of the random forest model, the system will adjust its parameters. Two parameters, the number of trees and the maximum depth of each tree, play a key role. The number of trees affects the comprehensive judgment ability of the model, while the maximum depth of each tree is related to the fitting degree of the model to the data. In the training process of the model, in order to accurately evaluate its performance, a cross-validation method will be adopted [11]. Through cross-validation, the performance of the model on different data subsets can be more comprehensively examined to avoid inaccurate evaluation results due to the chance of data division, and thus ensure that the model can run stably and efficiently in practical applications[12].

3.4. Experimental verification mode

In order to verify the performance and effectiveness of the computer network database protection system based on artificial intelligence, a simulation experiment is designed. This experiment simulates the real network environment and constructs a network architecture consisting of 3 subnets with 5 devices deployed in each subnet.

In terms of traffic Settings, the research team used traffic generators to make the network generate different types of traffic. Among them, the normal network traffic is maintained at 800Mbps, simulating the regular data transmission of the daily network. The experimental equipment also generated 200Mbps of attack traffic covering common types of network attacks to simulate complex and threatening network scenarios.

In the selection of classifier, this paper adopts random forest algorithm as the core classification method. In order to enable the algorithm to accurately identify normal and attack behaviors in the network, a large data set is used for training. The dataset contains 80,000 records, 70,000 of which are for normal network behavior and 10,000 of which are for attack behavior. A large amount of rich data provides sufficient learning samples for the random forest algorithm, so that it can judge all kinds of behaviors in the network more accurately, and then effectively protect the network security.

4. Analysis of experimental results

4.1. Analysis of measurement results

The performance of computer network database protection system under different experiment times is shown in Table 2.

Table 2. Performance test results of computer network database protection system

Attack type	Number of attacks	Detection rate	False alarm rate	Mean response time
SQL injection	30	91.20%	0.40%	310ms
DDoS	200	93.80%	1.60%	430ms
Unknown attack	10	84.00%	3.20%	510ms
Cross-site scripting	10	96.10%	1.90%	270ms

According to the data in Table 2, for SQL injection attacks, the system has a high detection rate and a relatively low false positive rate, which indicates that the system has a high accuracy and reliability when dealing with such common and harmful attacks. The average response time is 310ms, which can detect and respond to attacks in a short time, thus effectively reducing the damage caused by attacks.

In the face of DDoS attacks, the system also performed well, with a detection rate of 93.80%. Although the false positive rate increased slightly to 1.60%, considering that DDoS attacks are often accompanied by a large number of forged traffic and requests, the system can accurately identify the real attack behavior in the complex and changeable network environment, with good protection effect. The average response time of 430ms can also mitigate the impact of the attack to a certain extent.

For unknown attacks, the detection rate of the system is 84.00%, which is lower than that of known attack types, but considering the complexity and unpredictability of unknown attacks, this result is still acceptable. The false positive rate is 3.20%, and the average response time is 510ms. Although there is still some room for improvement, it also shows that the system still has a certain defense capability in the face of new attacks.

The detection rate of cross-site scripting attacks is the highest, reaching 96.10%, the false positive rate is 1.90%, and the average response time is only 270ms. This indicates that the system not only has high accuracy, but also responds quickly when dealing with such attacks, and can effectively block the attack behavior in time to protect the user's data security.

The memory usage of the computer network database protection system based on artificial intelligence is shown in Table 3. According to the test results in Table 3, the memory usage of the system remained stable during operation, and no obvious memory leakage or abnormal growth occurred. In the idle state, the system memory usage is small, and the memory usage will increase with the increase of network traffic and the detection of attack

behaviors. However, during the experiment, even in the face of high-intensity DDoS attacks, the system memory usage does not exceed 800MB, which indicates that the system has a good resource utilization efficiency and stability.

Table 3. Memory usage of computer network database protection system

Attack type	Average cpu usage	Memory usage
SQL injection	56%	58%
DDoS	68%	54%
Unknown attack	71%	70%
Cross-site scripting	50%	60%

The data transmission rate test results are shown in Table 4. According to the data in Table 4, under normal network environment, the data transmission rate of the system remains stable and can meet the daily network transmission requirements.

Table 4. Test results of data transmission rate of computer network database protection system

Transmission direction	Transmission rate（Mbps）
From client to server	80
From server to client	100

5. Conclusions

The computer network database protection system based on artificial intelligence presented in this paper shows remarkable results in dealing with various network attacks. Through the experimental verification of SQL injection, DDoS, unknown attack, cross-site scripting and other attack types, the system shows a high detection rate and good stability. Especially in the face of complex and changing network environment and new attack means, the system can still maintain a certain defense capability, effectively reducing network security risks. In addition, the system also performs well in terms of resource utilization, stable memory usage, and data transmission rates meet daily needs, ensuring efficient and stable network operation. Based on the above experimental data, this paper considers that the designed computer network database protection system based on artificial intelligence has high practical value and popularization significance.

Acknowledgement

Anhui Provincial Quality Engineering Project (2023): Research on teaching and practice of Intelligent control course based on OBE concept (2023jyxm0891); Natural Science Research Project for Anhui Universities (2022): Research on distance measurement of floating obstacles in water based on binocular vision (2022 AH0511987)

References

[1] Wu Jianjun. Research on Application of Big Data and Artificial Intelligence Technology in computer network system. Information Systems Engineering, 2024(8):63-66.

[2] ZHAO Bing, Xu Xin, Zhang Yue. Design of Computer network security defense system based on Artificial intelligence technology. Mobile Information, 2024, 46(5):155-157.

[3] Zhou Jianqing. Design and Implementation of Computer Network Security Protection System based on Artificial Intelligence Technology. Information and Computer, 2023, 35(4):202-204.

[4] Li Si, Liu Chaoyu. Discussion on the application of Artificial Intelligence in Computer network technology in the era of Big Data. Land Bridge Vision, 2023(1):46-48.

[5] Liu L. Design of Computer Network security defense System based on Artificial intelligence technology. Office automation, 2023, 28 (12) : 19-21.

[6] Wei Min. Research on Computer Network Information security Protection Mode based on Artificial Intelligence. Materials for Information

Recording, 2024, 25(11):130-132.

[7] Yang Yonghong. Research on Computer Network Security Defense System based on Artificial Intelligence Technology. Network space safety, 2024, 15 (4) : 306-309.

[8] LI Lulu. Research on Computer Network Security defense System based on Big Data and Artificial Intelligence Technology. Network security Technology and application, 2024(6):24-26.

[9] XU Chuyuan. Design and Analysis of Computer Network security defense System based on Big Data and Artificial Intelligence Technology. Digital Technology and Application, 2023, 41(7):216-218.

[10] Li Limin. Discussion on the construction of Network security protection System based on AI technology in the era of network intelligence. Information and Computer, 2023, 35(16):209-211.

[11] Wang Bowei, Lu Yu, Yang Hai, et al. Design and research of Network security defense System based on Artificial Intelligence. Journal of Computer Application Abstracts, 2023, 39(12):88-90.

[12] Chen Yangxi, Chen Dongfeng. Construction of Artificial Intelligence Technology in Cyberspace security defense. Chinese Science and Technology Journal Database (Abstract Edition) Engineering Technology, 2023(2):3.