Research on Network Information Security Defense System Based on Ai Big Data Analysis

Yining Ou

Santa Clara University, Santa Clara, Ca 95053, USA

ouyiningenid@163.com

Keywords: AI, Big data analysis, Network information, Security defense

Abstract: Owing to the constant progress of artificial intelligence big data technology, the research of network information security defense system is becoming increasingly vital. This article aims to study the network information security defense system based on AI big data analysis, and provide novel ideas and methods for enhancing the level of network information security defense. This paper analyzes the current application status of AI big data technology in the network information security defense system, points out the current problems and challenges, introduces the basic framework and components of a network information security defense system based on AI big data analysis, including network security data collection and storage, network security event detection and response, network security threat prediction and early warning, etc., and elaborates on the technical support in the network information security defense system based on AI big data analysis, including machine learning, deep learning, natural language processing, big data analysis, etc. These technologies can achieve rapid processing and analysis of large-scale network data, and perfect the response speed and accuracy of the network information security defense system.

1. Introduction

In the era of information and data explosion, computer information technology has played a vital role in various industries, providing convenience for users in various aspects. Owing to the widespread application of AI big data related technologies, such as cloud computing services and cloud storage, network information security issues have become increasingly concerned. However, the progress of early warning, security access, and network detection technologies related to network information security technology is currently lagging behind, and the network information security defense system urgently needs to be upgraded[1].

Therefore, we need to carry out research to enhance the network information security defense system, maintain and upgrade the information security system, and help AI big data better complete the exchange and storage of information, thereby bringing users a smoother, safer, and assured experience.

2. Analysis of the Current Situation of Network Information Security in AI Big Data Analysis

The current situation of network information security in the era of artificial intelligence and big data analysis is complex and challenging. The adoption of artificial intelligence and big data analysis enables enterprises to gain new insights and efficiency from data. It also brings new security challenges, requiring advanced security defense systems. Based on the characteristics of network information security defense systems in artificial intelligence and big data, we can discuss the following points.

First, increased complexity. Using artificial intelligence and big data analysis has led to an increase in the complexity of network security systems. To effectively prevent threats, enterprises need to deploy a range of security technologies, including firewalls, intrusion detection and prevention systems, anti-virus and anti-malware, and other advanced security tools. Second, advanced threats. The use of artificial intelligence and big data analytics has also spawned new

advanced threats. For instance, attackers can use artificial intelligence to automatically attack and evade detection. Enterprises need to stay ahead of these threats by continuously updating their security defense systems and investing in advanced security technologies. Third, the need for collaboration. Network security systems need to collaborate with each other and with other security systems to provide comprehensive protection and respond to threats. This requires the development of standards and protocols to enable interoperability between different security systems [2]. Fourth, skill gaps. In AI big data security, the skill gap is becoming increasingly large. Companies need to invest in training and development programs to ensure that their security personnel have the skills and knowledge necessary to effectively protect against threats. Fifth, regulatory compliance. Organizations are increasingly constrained by regulations that require them to protect the privacy and security of data. The design of cybersecurity systems needs to comply with these regulations, which may vary from jurisdiction to jurisdiction.

In summary, the current situation of network information security in the era of AI big data analysis is characterized by increased complexity, advanced threats, the need for collaboration, skill gaps, and regulatory compliance. To effectively address these challenges, enterprises need to deploy advanced security defense systems, including the latest technologies and best practices. In addition, they need to invest in training and development programs to ensure that their security personnel have the skills and knowledge required to effectively prevent threats [3].

3. Analysis on the Characteristics of Network Information Security Defense System in the Age of AI Big Data

3.1 Network Middle Layer in the Era of Artificial Intelligence and Big Data

In the era of artificial intelligence and big data, network information security defense systems are becoming increasingly sophisticated and complex. The following are some characteristics of these systems in the network middle layer. Real-time detection and response. With the increase in data volume and speed, network information security defense systems need to be able to detect threats in real time and react quickly to mitigate losses. This requires the use of artificial intelligence models that can analyze great amounts of data and make accurate predictions within seconds.

Firstly, starting from multi-dimensional analysis, network information security defense systems in artificial intelligence and big data need to be able to analyze data from multiple dimensions, such as network traffic, system logs, and user behavior. This requires the use of artificial intelligence models that can integrate and analyze data from different sources. Secondly, through automation and self-learning. To keep up with changing threats, network information security defense systems need to be able to adapt and learn from new data. This requires the use of artificial intelligence models that automate tasks and improve their performance over time. Finally, scalability and flexibility. As the amount of data increases, network information security defense systems need to be able to expand and adapt to changing needs. This requires the use of flexible architectures and cloud-based solutions that can handle large amounts of data and provide on-demand resources .

In addition, the role of collaboration and integration. Network information security defense systems need to collaborate and integrate with other security systems, such as firewalls, intrusion detection systems, and antivirus software. This requires the use of open standards and APIs for interoperability and data exchange.

In general, network information security defense systems are becoming more intelligent, adaptive, and collaborative. These systems are crucial for protecting sensitive data and critical infrastructure from network threats.

3.2 Network Application Layer in the Era of Ai Big Data

Network information security defense systems have become increasingly complex and sophisticated. In this case, it is essential to understand the characteristics of this system from the network application layer. Here are some key features:

First, intelligent detection and response. Network security systems increasingly use artificial

intelligence and machine learning algorithms to analyze network traffic and detect potential threats. These algorithms can learn from past events and adapt to novel threats, making them more effective in detecting and responding to attacks.

Second, big data analysis. Owing to the increasing amount and types of data generated by network applications, network security systems need to be able to process and analyze great amounts of data in real time. Big data analysis tools are used to extract meaningful insights from data and identify potential threats.

Third, multi-layer defense. Network security systems need to have multi-layer defense to prevent different types of threats. This includes the use of firewalls, intrusion detection and prevention systems, anti-virus and anti-malware, and other security technologies.

Fourth, active monitoring. Network security systems must be able to proactively monitor network traffic and identify potential threats before they cause harm. This involves using real-time monitoring tools to track network activity and identify abnormal behavior.

Fifth, collaboration. Network security systems must be able to collaborate with other systems and share information to enhance their effectiveness. This includes sharing threat intelligence and coordinating responses to attacks.

The network information security defense system in the era of artificial intelligence and big data is characterized by the ability to use advanced technologies such as machine learning and big data analysis to detect and respond to threats in real time. Their features also include multi-level defense methods, active monitoring, and collaboration with other security systems .

3.3 Basic Network Settings in the Age of AI Big Data

Network information security defense systems have become increasingly complex and sophisticated. In this case, it is essential to know the characteristics of this system from the perspective of network infrastructure settings, then set up the network foundation. The first is adaptive security. Network security systems need to be adaptive to cope with emerging threats. This requires the use of intelligent algorithms that can learn and adapt to new threats in real time. The second is network segmentation. Network segmentation is a vital feature of modern security defense systems. It involves dividing the network into smaller, more manageable parts to limit the impact of security vulnerabilities. Network segmentation also helps prevent attackers from moving laterally within the network. It is also vital to arouse attention to cloud security. With the increasing adoption of cloud computing, network security systems need to be able to protect cloud-based applications and data. This requires the use of specialized security tools and technologies designed for cloud environments. Finally, DevSecOps. DevSecOps is a development method that incorporates security into the software development process. This approach has become increasingly vital to ensure that security is incorporated into every aspect of network infrastructure.

Moreover, focus on threat intelligence. Threat intelligence is crucial in the era of artificial intelligence and big data. It involves using specialized tools and techniques to identify and analyze potential threats, and sharing this information with other security systems to enhance their effectiveness.

The characteristics of network information security defense systems in the era of artificial intelligence and big data are the ability to use advanced technologies such as machine learning and big data analysis to detect and respond to threats in real time. They also feature adaptive security, network segmentation, cloud security, DevSecOps, and threat intelligence capabilities designed to provide comprehensive protection for modern network infrastructure.

4. Research and Application of Network Information Security Defense System Based on AI Big Data Analysis

4.1 Design Steps of Network Information Security Defense System for AI Big Data Analysis

Designing a network information security defense system based on AI big data analysis is a complex task that requires careful planning, implementation, and testing. The following are some

general steps to follow to get started, As shown in Fig. 1.

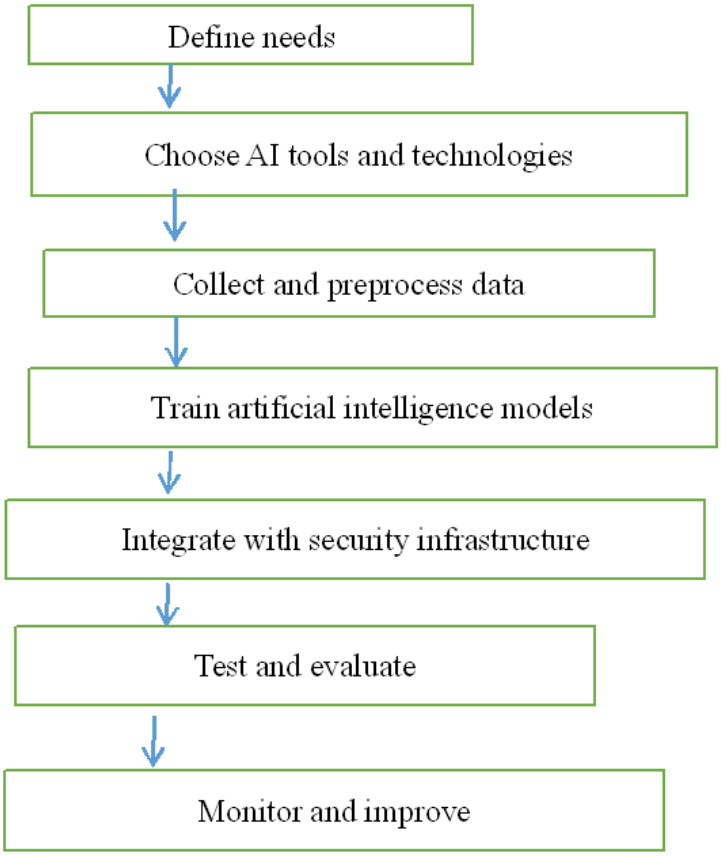

Fig.1 Design Steps of Network Information Security Defense System

Define requirements. First, determine the requirements for your network information security defense system, that is, what threats are you protecting. Next, collect the data that needs to be analyzed, and define what alerts and reports to generate.

Choose artificial intelligence tools and technologies. There are several AI tools and technologies available for network security, such as machine learning, deep learning, natural language processing, and data mining. Select the technology that best suits the needs of the environment.

Collect and preprocess data. Collect necessary data from various sources, such as logs, network traffic, and security events. Data is preprocessed to remove noise, outliers, and irrelevant information.

Train artificial intelligence models. Use pre-processed data to train artificial intelligence models. You may need to experiment with different algorithms, hyperparameters, and feature selection techniques to achieve optimal performance.

Integrate with security infrastructure. Combine artificial intelligence models with your security infrastructure, such as firewalls, intrusion detection systems, and antivirus software. Define rules and policies for how AI models should interact with security infrastructure.

Test and evaluate. Thoroughly test the system to ensure that it meets requirements and performs as expected. Evaluate performance indicators such as accuracy, false positive, false negative, and response time.

Monitor and improve. Continuously monitor the system for new threats and vulnerabilities. Collect feedback from users and use it to gradually improve the system.

4.2 Design of Network Information Security Defense System for AI Big Data Analysis

Example:

```
import pandas as pd
from sklearn. model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier
```

```
#Read Dataset
data = pd. read_csv('network_traffic.csv')
#Data preprocessing
data['label'] = data['label'].apply(lambda x: 1 if x == 'attack' else 0)
X = data. drop(['label'], axis=1)
y = data['label']
#Divide training sets and test sets
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2)
#Construct a random forest classifier
clf = RandomForestClassifier(n_estimators=100)
clf. fit(X_train, y_train)
#Evaluate model performance on a test set
accuracy = clf. score(X_test, y_test)
print('Accuracy:', accuracy)
```

The above code example is written in Python, using the Pandas library to read and process data sets, and using the random forest classifier algorithm from the Scikit-learn library for training and prediction. The specific steps include:

Read Dataset: To read a dataset from a CSV file, read_ Csv() function in the Pandas library can be used.

Data preprocessing: Perform some preprocessing operations on data, such as converting attack tags to binary tags, deleting unnecessary columns, and so on.

Divide training sets and test sets: Divide the data set into training sets and test sets, and the train_ test_ Split () function in the Scikit-learn library can be used.

Construct a model: Use a random forest classifier algorithm to build a model, and use training sets to train it.

Evaluate model performance on a test set: Use the test set to evaluate the trained model and calculate performance indicators such as accuracy.

It should be noted that the specific implementation method also needs to be adjusted and modified according to actual needs. The network information security defense system for AI big data analysis usually involves more complex algorithms and architectures, so it is essential to select appropriate algorithms and tools in combination with specific scenarios and requirements in actual implementation.

4.3 Application of Network Information Security Defense Architecture Model for AI Big Data Analysis

Designing a network information security defense system based on AI big data analysis does require specific system code and specific models. Here are some steps to follow.

First, determine the data source. Determine the type of data that will be collected and analyzed. This may include network traffic data, log files, and security alerts.

Second, preprocess data. Preprocess the data to remove noise and irrelevant information and convert it into a format suitable for analysis. This may include tasks such as data cleansing, data transformation, and data normalization.

Third, choose an artificial intelligence model. Choose the AI model that best suits the specific security task you want to accomplish. For instance, you can use machine learning models to detect anomalies in network traffic, or use natural language processing models to analyze security event reports.

Fourth, train model. Training artificial intelligence models on preprocessed data involves using a training set to teach models how to recognize patterns and make predictions. You may need to experiment with different algorithms and hyperparameters to find the best model for your specific needs.

Fifth, integrate model. Integrate trained models into your security infrastructure, such as intrusion detection systems, firewalls, and antivirus software. And then define rules and policies for

how the model should interact with the security infrastructure.

Sixth, test and evaluate. Test the system to ensure that its performance meets expectations. Evaluate performance indicators such as accuracy, recall, and false alarm rates.

Seventh, monitor and improve. Continuously monitor the system for new threats and vulnerabilities. Collect feedback from users and use it to gradually improve the system.

When it comes to specific system code and models, it will depend on the specific AI tools and technologies you choose, as well as the programming language and framework you prefer. Some examples of AI models commonly used for network security include:

Artificial Neural Networks (ANNs). ANNs can be used for tasks such as intrusion detection and network traffic classification.

Decision tree. Decision trees can be used for tasks such as anomaly detection and intrusion detection.

Support Vector Machines (SVMs). Support vector machines can be used for tasks such as malware detection and network intrusion detection.

Random forest. Random forests can be used for tasks such as intrusion detection and classification of network traffic.

There are also many programming languages and frameworks available for implementing artificial intelligence models, such as Python, R, and TensorFlow. It is vital to choose the language and framework that best suits the needs and expertise of the environment.

5. Conclusion

In the context of artificial intelligence, big data, and cloud computing, the situation of network information security has undergone new changes, with the behavior of intruders becoming more diverse and covert, which requires continuous upgrading and maintenance of the network information security defense system. In the artificial intelligence big data analysis environment, network intrusion behaviors will also leave richer log information, which also provides more data and methods for network security monitoring and management. In the future, in the environment of AI big data analysis, the computer network security information defense system can better demonstrate its own functions, and can be well promoted and applied.

References

[1] Li Zhi. Security Technology Education and Teaching Strategies in the Network Information Age: A Review of Information Security Technology and Applications. Journal of Safety and Environment, vol.22, no.3, pp.1699-1700, 2022.

[2] Xue Laijun. Network Information Security Encryption Method Based on Improved E-C. Journal of Taiyuan Normal University (Natural Science Edition), vol.21, no.2, pp.48-50, 2022.

[3] Niu Geng. Information security detection method for cellular optical fiber sensor networks based on fuzzy matching. Journal of Lasers, vol.43, no.6, pp.206-210, 2022.