Research on Computer Network Vulnerability Scanning Technology Based on Deep Learning Technology under the Background of Large Data

Lv Haitao[1], He Rongjie[2], Liu Guixiang[1,*]

[1]Modern Educational Technology Center, Harbin Finance University, Harbin 150030, Heilongjiang, China

[2]Harbin Finance University Library, Harbin 150030, Heilongjiang, China

Keywords: Big Data; Deep Learning; Network Vulnerability Scanning Technology

Abstract: The rapid development of computer not only brings convenience to people's lives, but also has many hidden dangers. The hacker attack is one of the most important problems. It is also because of the rapid development of hacker attack technology that people pay more and more attention to the security of the network. This paper presents the concept of deep learning, a sub-domain of large data and machine learning, and expounds the important role of deep learning in acquiring valuable information in large data. This paper studies the application of modern big data method in the field of computer network vulnerability scanning technology, and proposes a computer network vulnerability scanning technology based on deep learning. The online dynamic prediction of the system is carried out through fault model training, fault feature recognition, and fault evolution law acquisition, thereby improving the security of the computer network.

1. Introduction

The Internet is an open network platform. Many people can transmit all kinds of information on the network platform, which brings convenience to the network office and promotes the sharing of information resources. But it also means that the network has certain vulnerability and potential threats [1]. Therefore, in the actual application of computer networks, people must strengthen the use of computer security vulnerability scanning technology, and do a good job of computer network security protection. At present, in addition to the security mechanism of the computer itself, the main security measures of the computer network are firewalls. With the development of hacker attack technology, system vulnerabilities are more and more exposed. The weakness of the firewall makes it impossible for many attacks, especially for internal attacks, it is helpless [2]. With the development of technologies such as the Internet of Things and cloud computing and the advent of the era of big data, the global network security situation is even more severe. Therefore, it is an important means to strengthen network security by analyzing the large-volume data of the network through machine learning to identify intrusion behavior.

At present, there are many researches on target detection based on deep learning. The application is very effective in target detection, but most of the research is only in the laboratory stage. The depth model has large parameters, the model volume is large, the detection speed is slow, and the hardware requirements are met. High, poor real-time [3]. For people, how to effectively use big data and get valuable information from it is a serious challenge. Machine learning, especially in-depth learning, as well as progressive computing power, will become a key to the opening of a large data repository. In this paper, a fault prediction scheme based on deep learning is proposed. The deep learning algorithm is used to process the massive fault data obtained from equipment condition monitoring and test verification, and the fault prediction is carried out through fault model training, fault feature recognition and fault evolution rule acquisition.

2. Computer Network Vulnerability Scanning

Deep learning architecture is composed of multi-layer non-linear operation units. Each lower level output serves as the input of the higher level. It can learn effective feature representation from a large

  DOI: 10.25236/isaicn.2019.041

number of input data. The learned higher-order representation contains many structural information of input data. Deep learning requires very little manual engineering, and can easily benefit from the increase in available computing power and data volume, both of which contribute to further learning to achieve more success [4]. Vulnerability, also known as vulnerability, is a defect in the implementation of software, hardware and protocol or system strategy of computer system. Once the flaws between the network and the host are found, the vulnerabilities will multiply into the virtual world and bring harm to the computer and the information stored on it. Computer security vulnerability scanning technology is an important protection method for computer networks, which can detect network devices and terminal systems in computer networks [5]. Vulnerability scanning software can enhance the security of the network system, but it can also provide the convenience for the criminals to enter the network. The user uses the vulnerability scanning software to protect the system, the hacker uses the vulnerability scanning to invade the system, and the administrator uses the vulnerability scanning to perform security protection. Therefore, it is not feasible to rely entirely on vulnerability scanning software.

Vulnerabilities fall into two broad categories: application vulnerabilities and operating system vulnerabilities. Application software vulnerabilities are mainly vulnerabilities in network service software provided by the system, such as WWW service vulnerabilities, FTP service vulnerabilities, SMTP service vulnerabilities, Telnet service vulnerabilities, etc. The main shield of the computer at this stage of protection attacks is the firewall, and the passive defense method allows hackers to attack in a more advanced way. The more advanced the hacker's technology, the worse the quality of the firewall. Deep learning uses multi-layer artificial neural networks to learn training from big data sets, and finally to intelligently identify and accurately predict new data samples. Because the target may appear in any position of the image, and the size and aspect ratio of the target are uncertain, the most commonly used method is to use the sliding window strategy to traverse the measured samples. In order to achieve accuracy, different scales and different aspect ratios need to be set. In supervised learning, the input data for model learning is called training data, and the data that needs to be input into the model for testing is called test data. The training data has its own label or result. At the same time, another one-way flow of information flows from the hidden unit to the output unit. Sometimes RNN breaks the restriction of the latter and guides the information flow back to the hidden unit from the output unit. However, different vulnerabilities require different response data and signatures. Only matching response data signatures can form network vulnerabilities. Therefore, scanning the signature becomes an important means to ensure network security.

Network-based vulnerability scanning is to record the response given by the target host by remotely detecting the services of different ports of the target host TCP/IP. In this way, you can collect a variety of information about many target hosts. Actively check the computer system and the computer network, and maintain the computer through various methods such as pre-checking and simulated attack, so as to find the loopholes of the computer and repair it, and the device that can effectively reduce the interest can be visually compared to the service window. The training data and the test data are loaded into the classifier of the model of the present invention, wherein the training data enters the training module of the deep neural network classifier, and the test data enters the test module of the deep neural network classifier. Data acquisition is mainly feedback from external environment, and the model must respond to these feedback data. Feedback in reinforcement learning comes from external environment, and parameters are adjusted dynamically to achieve the goal of reinforcement signal. However, it is difficult to improve the processing speed by parallel operation when dealing with large data. Deep learning algorithms usually involve large-scale hidden neurons and millions of parameters, which can process massive data and train complex models. In the process of automatic detection, it is necessary to know whether there are loopholes in the host's operating system, programs and servers through the host's response, so as to realize the detection of network loopholes.

3. Application of Computer Network Security Vulnerability Scanning Technology

As a traditional scanning method, active scanning is sent automatically by computer, which can

play a role of network security protection. The scanning speed is relatively fast, and accurate information can be obtained. The shortcoming is that it will leave scanning traces and be easy to be found. From the current situation, many computer networks will set user names and login passwords, so that the operation rights of the network will be assigned to different users. If people crack the user names, they can obtain access rights of the network, making network security difficult to guarantee. We can see that many application networks have user names and passwords, but these passwords are too simple. Intrusion can easily crack passwords, thus destroying the system and obtaining the operation rights of these services. These may be the negligence of network managers. According to the relevant settings in the user configuration console section, the scan engine first assembles the corresponding data packet and then sends it to the target system, and then compares the received response data packet of the target system with the vulnerability feature in the vulnerability database. To determine if the selected vulnerability exists. The training data is trained by the deep neural network classifier to obtain valid results, then the test data is loaded, and then the test data set categories are predicted based on the training effective results. The prediction result is obtained, that is, the classification prediction process is completed. When the customer requests that the service equipment can exceed the range that the service equipment can withstand, the customer must wait, which is the reason for the queuing phenomenon. The relationship between the number of service devices and customer needs can determine the quality of the service to a certain extent.

The features used in traditional target detection algorithms are all designed by hand and rely too much on manual tuning. The quality of the algorithm depends entirely on the prior knowledge of the feature designer. Moreover, traditional hand-designed features work better only when solving a specific category of target recognition problems. With the development of machine learning and deep learning theory, machine learning-based methods have become the development trend of equipment failure prediction technology. In the case of composite faults, each fault interacts with the system, and the fault modeling and theoretical analysis of the composite fault cannot be performed using the model features. The use of convolutional neural networks in large-scale data processing uses a multi-core GPU. The number of threads needed in the training process is determined by the size of the selected filter. User names and passwords of network users are used to control the reading of mail. Before scanning, the user identification document and password document should be established, the instructions should be sent to the target host, and then the response information should be judged, so that the weak user name and password can be found. When scanning vulnerabilities, user identification and password documents are established, and login passwords and user identification are stored in the documents, which can be updated in time. But the speed of scanning is slow. If the target of scanning can generate the object of network traffic, otherwise it can not be scanned out. Generally speaking, active and passive scanning needs to be optimized, which will greatly improve its function.

Encryption mechanism in communication between scanning server and target host. Generally, the communication data packets between the console and the scanning server are encrypted, but the communication data packets between the scanning server and the target host are not encrypted. In the process of searching for the optimal subset from the feature space of a data set, redundant features and irrelevant features will be removed from the original feature set, thus retaining the features that determine the distinction between data features, which can greatly reduce the dimensionality of sample data and improve the efficiency of training learning models. With the continuous expansion of data scale, the input and output of deep learning model may increase exponentially, and the dimension of data will also increase continuously, which directly leads to the increase of operation time of deep learning model and the complexity of model. When the vulnerability is scanned, the target port is connected to determine whether the protocol is in the authentication state. If the failure or the wrong information indicates that the identifier is unavailable, if all the results are useful information, the identity authentication is passed. In order to make up for this loophole, it is necessary to lengthen the length and complexity of the password, making it more difficult for the criminals to use. It can also be changed by the administrator username, making it more difficult to be guessed by unauthorized users. In order to improve the security of the network, reduce the frequency of such

vulnerabilities, expand the length of the password, increase the complexity of the password, and improve the difficulty of cracking the criminals. In addition, you can make changes with an administrator username, which is more secure.

4. Conclusions

In general, there are many more computer network security technologies. This article only discusses the commonly used network security protection technology. This technology is a complex technology, which involves not only computer science, network information technology, but also communication. Technical and psychological knowledge. This paper is difficult to analyze the interaction of each fault in the case of composite faults in the case of conventional forecasting methods. At the same time, it introduces the application and challenges of each model in the big data environment and the development prospects of deep learning in the context of big data. Using the massive data obtained from equipment condition monitoring and test verification, the deep learning algorithm is combined with the characteristics of equipment fault data to form a dynamic fault prediction technology based on deep learning. One of the important means to prevent computer network vulnerabilities is to scan vulnerabilities, consolidate computer hardware and software systems, on the one hand, prevent the emergence of vulnerabilities, on the other hand, deal with existing vulnerabilities, and do a good job of security remedies to improve the security of computer networks. As far as the current vulnerability scanning technology is concerned, automated vulnerability scanning can not be fully realized, and new problems will emerge, so the network vulnerability scanning technology still needs further research and improvement.

References

[1] Chen L, Chen X, Jiang J, et al. Research and practice of dynamic network security architecture for IaaS platforms. Tsinghua Science and Technology, 2014, 19(5):496-507.

[2] Chen H Y. The Research of Computer Complex Network Reliability Evaluation Method Based on GABP Algorithm. Applied Mechanics and Materials, 2014, 556-562(556-562):4.

[3] Zhang Y P. Design for the Application Layer of Network Security Solutions. Advanced Materials Research, 2014, 998-999:1113-1116.

[4] Choi Y H, Park M W, Eom J H, et al. Dynamic binary analyzer for scanning vulnerabilities with taint analysis. Multimedia Tools and Applications, 2015, 74(7):2301-2320.

[5] Johnson L. Chapter 10. System and Network Assessments. Security Controls Evaluation Testing & Assessment Handbook, 2016:499-530.