Network Information Security Protection Technology Based on Big Data Technology

Chao WANG, Xiaohu Wang, Jiahan Dong, Guangxin Guo, Tianyu Ren
State Grid Beijing Electricpower Company Electric Power Research Institute, Beijing, China

Keywords: Big data technology, Network information security, Information security protection, Data mining

Abstract: The construction of network information security is not only the development security of network information technology in the era of big data, but also an important guarantee to ensure the safety and order of network environment. Based on this, this paper studies the network information security protection technology based on big data technology. In this paper, we first understand and analyze the current situation of network information security, and summarize the hidden dangers of network information security under the background of data. Secondly, on the basis of data mining in big data technology, this paper proposes a network information security protection technology based on big data technology. In order to study the network information security protection technology based on big data proposed in this paper, the simulation experiment is carried out on the simulation platform, and the method is compared with the traditional network protection technology and the big data based NAT network security protection technology, and the network defense ability and attack index are studied. The results show that the network defense capability of traditional network protection technology is 72%, and the attack index is 32%. The network defense ability of firewall network security protection technology based on big data is 89%, and the attack index is 13%. The network defense ability of NAT network security protection technology based on big data is 91% and the attack index is 17%. From the simulation results, we can see that the performance of network information security protection technology based on big data is better, and can play a better role in network information security protection.

1. Introduction

With the further popularization and development of network technology, it also brings many security risks to the society, among which the most important point is whether the network information is safe \[1-2\]. With the rise of cloud computing, online payment, Internet of things and other industries, the importance of big data has gradually emerged. It is precisely because of the strong support of national policies that the era of big data has come \[3-4\].

As the strong backing of the Internet industry, big data provides many unexpected conveniences for the Internet industry \[5-6\]. However, the society's attention and deep development of big data technology and people's constant pursuit of Internet speed have led to frequent network information leakage incidents in the era of big data \[7\]. We know that once the network information problems occur, it may lead to the normal operation of the computer system, or even the phenomenon of paralysis, resulting in irreparable economic losses of network users. Therefore, it is of great significance to explore the network information security protection technology in the era of big data.

This paper expounds the network information security and data mining, summarizes and analyzes the network information security problems under the background of big data, and proposes a network information security protection technology based on big data technology on the basis of data mining, and puts forward corresponding protection measures for network information security protection. In order to verify the performance of the network information security protection technology based on big data proposed in this paper, the simulation experiment is carried out on the network security simulation platform. The experimental results show that the protection technology proposed in this paper has excellent performance and can play a good role in network information
security protection.

2. Network Information Security and Data Mining

2.1 Network Information Security

Network information security is divided into network security and information security. Network security includes system security, that is, hardware platform, operating system and application software; operation service security is to ensure the continuity and efficiency of services. Information security mainly refers to data security, including data encryption, backup, program, etc. Network information security mainly refers to the following four aspects:

The fourth aspect is data security, that is, the security of data storage and circulation in the network.

2.2 Data Mining

Data mining is mainly from a large number of data search, mining useful information, so as to provide support for decision-making, widely used in various fields. In recent years, with the development of computer network technology, data mining technology is widely used in the field of network information security.

Data mining model is the most important part of data mining, there are many methods of data mining modeling, this paper uses the logistic regression model.

Logistic regression model is based on linear regression, through the application of a logical function, the introduction of nonlinear factors, so as to solve the classification problem.

The general linear regression model is as follows:

$$f(x) = \omega_0 + \omega_1 x_1 + \omega_2 x_2 +... + \omega_d x_d + b = \omega^T x + b \quad (1)$$

The value of parameter $\omega$ is estimated based on the minimum loss function. The loss function is constructed and solved by maximum likelihood estimation and least square method. If $g^{-1}(\cdot)$ is a monotone differentiable function, a generalized linear model is obtained.

$$y = g^{-1}(\omega^T x + b) \quad (2)$$

The output value of linear regression is real value, while the expected output value of binary task is 0 or 1. To do this, we need to find a connection function to convert the output value so that the output value is only 0 or 1. The ideal connection function is to use the unit step function, but its property is not good, so we need to find a substitute function. Therefore, it is often used to replace the monotone differentiable and arbitrary order derivative logarithmic probability function.

$$y = \frac{1}{1+e^z} \quad (3)$$

3. Simulation Platform Construction and Simulation Experiment Design

3.1 Construction of Network Security Simulation Platform

Through the research of Network Security Modeling and simulation technology, as well as the software and hardware architecture of the platform, this paper establishes an open network security simulation and simulation platform, which provides interfaces with real devices, real systems, other simulation tools, and other knowledge bases. It supports the following five levels of network security simulation.

1) Equipment level simulation;
2) Simulation of main network attacks;
3) Simulation of network scheme;
4) Simulation of complex network environment;
5) Simulation against network environment.

3.2 Experimental Simulation Design
In order to verify the effectiveness of the proposed method, we select the traditional network protection technology and the firewall network security protection technology based on big data as the contrast, and conduct the simulation experiment, and evaluate the three network security protection technologies from two aspects of network security defense ability and attack index.

4. Network Information Security Protection Technology Based on Big Data Technology

4.1 Analysis of Network Information Security under the Background of Big Data

This paper analyzes the network information security problems under the background of big data, and the results are shown in Figure. This paper summarizes the network information security problems under the background of big data, and sums up some main network information security hidden dangers at present. As can be seen from Figure 1, the existing network information security risks mainly include the security problems of the network system itself, the invasion of hackers, the imperfection of network information security management system, the threat of information pollution, the citizens' poor awareness of network information security and the hidden danger of computer viruses. This is analyzed in detail below.

4.1.1 Security of Network System (13.1%)

In most cases, there are problems in the initial design of the network system, and even some problems are inevitable. Therefore, most of the network security problems we see are caused by the problems of the network system itself.

4.1.2 Hacking (22.4%)

Hacker's invasion is also one of the factors that threaten the network information security. Hackers are proficient in computer technology and computer network technology.

4.1.3 Imperfect Network Information Security Management System (9.75%)

In today's information age and big data era, there are many problems in the network information security management system. In the process of governance of network information security, the government of our country has not promoted the innovation of network information technology, and has not made much progress in the core technology. The management system of network information security in China is not perfect.

4.1.4 The Threat of Information Pollution (25.5%)

Information pollution is that network information is mixed with some false and unhealthy information, which has a negative impact on our work and study. At present, our country lacks some effective measures to control the network. There are a lot of junk information in the network that can't be deleted in time, resulting in certain information pollution. As a platform, the network is open and shared, which determines that it is difficult for us to better and more effectively protect the original works. The plagiarism and plagiarism caused by it have become a common phenomenon, and a large number of similar network information has been formed on the network, which undoubtedly increases the difficulty for our government to govern the network information.

4.1.5 Citizens' Awareness of Network Information Security Was Poor (13.4%)

Our personal users in the process of using the network, many people's security awareness is poor.

4.1.6 Hidden Danger of Computer Virus (15.9%)

Computer virus has a fatal impact on the computer, it can destroy the computer security system, so that all kinds of information in the computer are destroyed and leaked.

4.2 Analysis of Network Information Security Protection Technology Based on Big Data Technology

4.2.1 Protective Measures
Aiming at the problem of network information security under the background of big data, this paper proposes network information security protection technology based on big data technology on the basis of data mining, and puts forward a series of protection measures, as shown in Table 1.

<table>
<thead>
<tr>
<th>Network security protection measures</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay attention to account security protection</td>
<td>Ensure the safety of funds</td>
</tr>
<tr>
<td>Encryption of data preservation and circulation</td>
<td>Ensure the security of information circulation</td>
</tr>
<tr>
<td>Firewall technology</td>
<td>Prevent virus invasion</td>
</tr>
<tr>
<td>NAT Technology</td>
<td>Prevent information leakage</td>
</tr>
<tr>
<td>Improve the network governance system</td>
<td>Guarantee the security of network environment</td>
</tr>
<tr>
<td>Enhance network security awareness</td>
<td>Avoid network pitfalls</td>
</tr>
</tbody>
</table>

It can be seen from Table 1 that in the context of big data, to ensure information security, first of all, we should pay attention to account security protection to ensure the security of funds. Secondly, the encryption of data preservation and circulation ensures the security of information circulation.

4.2.1.1. Pay Attention to Account Security Protection

Although the threat of network information security in the era of big data comes from all directions, under the promotion of economic interests, the most important threat is from the bank accounts of ordinary people and online electronic payment. In the process of real-time online payment, some criminals will make some fake payment websites, or inject illegal advertisements into the payment websites to capture users' payment accounts and passwords. Therefore, we should pay attention to the security protection of accounts.

4.2.1.2. Encryption of Data Preservation and Circulation

Because big data needs to be circulated, it can only be displayed through the processing and rendering of some professionals. Therefore, big data has two obvious characteristics: preservation and circulation.

4.2.1.3. Firewall Technology

Network information needs some technologies to provide security in the process of interaction, among which firewall technology plays an important role.

4.2.1.4. Nat Technology

NAT technology is also the network address translation technology, the main purpose is to effectively transform private address and public address.

4.2.1.5. Improve the Network Governance System

Speeding up the establishment and improvement of the network comprehensive governance system will help to create a clean and clean network space. We should enhance the guidance of network public opinion, improve the handling mechanism of major online public opinions, focus on the governance of network ecology, strengthen the self-discipline of the Internet industry, and severely crack down on network crimes. We will coordinate all fields related to network security and information development, and lead the network governance model and governance capacity in China.

4.2.1.6. Enhance Network Security Awareness

In the big data environment, almost all social groups rely on the network to live and work. People must improve their awareness of network security, enrich their network security knowledge, and avoid falling into the network “trap” set by criminals.

4.2.2 Performance Analysis of Network Information Security Protection Technology Based on Big Data

In order to study the performance of network information security protection technology based
on big data proposed in this paper, simulation experiments are carried out on the network security simulation platform, and the experimental results are shown in Table 2.

Table 2 Technical Performance of Network Security Protection Based on Big Data

<table>
<thead>
<tr>
<th>Safety performance</th>
<th>Network defense capability</th>
<th>Attack index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional network security protection technology</td>
<td>72%</td>
<td>32%</td>
</tr>
<tr>
<td>Firewall network security protection technology based on big data</td>
<td>89%</td>
<td>13%</td>
</tr>
<tr>
<td>NAT network security protection technology based on big data</td>
<td>91%</td>
<td>17%</td>
</tr>
</tbody>
</table>

As can be seen from Table 2 and Figure 2, this paper conducted three experimental tests on the network security simulation platform. Among them, the network defense ability of traditional network protection technology is 72%, and the attack index is 32%. The network defense ability of firewall network security protection technology based on big data is 89%, and the attack index is 13%. The network defense of NAT network security protection technology based on big data is 91%, and the attack index is 17%. Thus, the network security defense capability based on big data is stronger, the attack index is lower, and the network information security protection capability is stronger.

5. Conclusions

On the basis of data mining, this paper proposes a network information security protection technology based on big data technology, and verifies the effectiveness of the proposed method through simulation experiments. This paper believes that in the era of big data, we should make full use of the advantages of big data to support other traditional industries. At the same time, we should also see the problems that may arise in the development of big data. However, we should not give up because of choking. We should do a good job in the network information security protection in the era of big data, and escort the development of technology in the era of big data. At the same time, we should also take advantage of the opportunity of big data era to rectify the computer network industry and create a beautiful computer security information body.

References


