Journal of Artificial Intelligence Practice (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2022.050309
ISSN 2371-8412 Vol. 5 Num. 3

Computer Network Security in the Background of Big Data

Dexi Chen[1,2,*], Juan Wu[1,2], Haiqing Liu[3]

[1]*School of Computer and Big Data, Jining Normal University, Wulanchabu, Inner Mongolia, China*
[2]*Philippine Christian University Center for International Education, Manila, Philippine*
[3]*Jining District Experimental Middle School, Wulanchabu, Inner Mongolia, China*
64305952@qq.com
[*]*Corresponding author*

Keywords: Big Data, Computer Network, Network Security, Security Precautions

Abstract: In the age of big data(BD), with the rapid growth of computer network technology, it plays an indispensable role in people's life. However, due to the immaturity of China's Internet security precautions, loopholes, hacker attacks and other factors, user information and property have been affected, causing serious losses. From the perspective of computer network crime, this paper mainly analyzes the shortcomings of current domestic laws, regulations and policies in this area and the solutions to them, studies and puts forward some suggestions and countermeasures, and discusses the current situation of computer network security(CNS) in the context of BD. After that, we studied the application of encryption algorithm in the context of BD, designed a CNS framework based on the algorithm, and then tested the security of the algorithm. The final test results show that the security protection of BD based encryption algorithm for data is more than 90%, which shows that the CNS requirements can meet the requirements.

1. Introduction

With the continuous growth of information technology, the network has also become an indispensable part of people's daily life[1-2]. The number of Internet users in China has continued to increase in recent years. Among them, smart phones are representative. These mobile terminals have gradually replaced traditional personal computers and office equipment and occupied most of the time. With the popularization of mobile phones, tablets and other portable communication tools and the rapid progress of wireless network access technology, mobile networks have developed rapidly and been widely used, which brings great challenges to CNS [3-4].

Many scholars have done some research on CNS. Some foreign researchers have proposed that CNS is a complex system engineering, involving a lot of discipline knowledge. Foreign scholars have conducted in-depth analysis and discussion on the problems of computer networks in the age of BD [5-6]. China started relatively late in this field. At present, there is no complete systematic and normative laws and regulations on Internet technology in China to ensure its security, confidentiality and other basic concepts and related content. At the same time, some people believe that hacker attacks will bring huge losses to enterprises and even cause the leakage of state secrets.

Therefore, it is urgent to study Internet security precautions. Some scholars use BD to analyze and mine the problems in user behavior information [7-8]. They put forward some suggestions from different aspects to solve these shortcomings. At the same time, they also found that hacker intrusion is an improper means that leads to a series of problems such as personal privacy disclosure and increased risk of property loss. They also pointed out that in order to effectively avoid attacks, it is necessary to improve the CNS technology prevention level and strengthen the management and protection measures for computer viruses, Trojan horses, malicious programs and other security threats. Therefore, based on BD technology, this paper studies CNS.

With the arrival of the BD era, CNS has also ushered in new opportunities and challenges. How to cope with these new changes has become the focus of current research. This paper first describes the exploration and analysis of CNS issues in China under the background of the rapid growth of the Internet. Then it introduces the shortcomings and areas that need to be improved in the current domestic laws, regulations and technical standards in this field. Finally, it puts forward corresponding countermeasures and suggestions to prevent the emergence and outbreak of CNS risks in the era of BD, I hope it can provide reference value for relevant departments.

2. Discussion on CNS in the Background of BD

2.1 CNS

In the age of BD, CNS issues are also increasingly prominent. Due to the wanton intrusion of hackers, some important information was leaked to users. At present, CNS mainly aims at the management of people, machines and space, and encrypts data[9-10]. Therefore, it is necessary to prevent and manage them. At the same time, technical means can be used to improve the ability to resist viruses, trojans and other attacks, as well as to protect the system and confidential files from leakage and other measures to effectively solve the above series of problems. Hackers may cause system paralysis or other serious losses after using various means to attack the Internet. It is an effective measure to protect network security by setting communication protocols between internal servers and external devices to realize intrusion detection systems and isolate the relationship between computers and the external environment. First, physical network cards can be used to control access and prevent illegal users from entering. In terms of CNS, it is mainly aimed at network security technology prevention. Second, we should strengthen the management of Internet users. Through the establishment of sound laws and regulations to restrict individuals and enterprises to use others' information. Third, it is necessary to improve the self-protection capability of the computer system, strengthen the construction of equipment and facilities such as firewalls, strengthen the research and growth of network security protection software, and increase the investment in hardware equipment to prevent hacker intrusion and information leakage. The security of computer network mainly refers to that the network information data is not easy to be deleted, damaged or lost in the process of transmission and storage, so as to ensure that information resources will not be disclosed and data integrity will be guaranteed. For users, it is necessary to provide sufficient storage devices with good quality and excellent performance to store such information; In addition, important infrastructure such as servers should be well configured to ensure the safe operation, normal use and maintenance of the network [11-12].

2.2 Impact of BD on Computer Security

The emergence of BD has a huge impact on CNS. The age of BD has brought us many features such as convenience, rapidity, high openness and a large amount of information. At the same time, it has a series of characteristics such as very extensive distributed characteristics and diversity

characteristics. Due to the openness, sharing and rapid propagation of the Internet, a large amount of information is intercepted and mined in the transmission process. And hackers use these technical means to steal confidential documents or tamper with important databases. With the growth of the Internet, CNS has also been greatly affected. With hacker technology and network viruses causing more and more losses to people, these hazards are huge and difficult to solve. For example, obtaining personal privacy by illegally intercepting user account passwords, stealing mobile phone numbers and communication addresses stored on APP software by using Trojan programs, and uploading them to other websites or public network servers to obtain others' login permission are all serious hazards caused by BD security issues. Hackers carry out malicious attacks in various ways. In some websites, you can see that users log in as "Trojan horses". These accounts and passwords are protected objects. For the server, it is a means that no one is allowed to access and share resources to steal information, delete or disclose confidential data, destroy trade secrets and other acts will bring huge losses to the computer network. Therefore, in order to effectively solve the security problems caused by BD, we must strengthen its preventive measures.

2.3 BD Technology

Big data technology is an important field of CNS. In today's society, with the rapid growth of the Internet, people pay more and more attention to information resources and services. With the advent of the BD era and the continuous progress of information technology. The traditional sense of CNS is also facing new challenges. First, the information storage mode has changed. Now, most of them use hard disk as the main storage medium for storage, management, maintenance and other operations. Digital storage mode is used to achieve information sharing and utilization. Second, the transmission speed is reduced, resulting in security degradation and confidentiality problems. Big data technology is an important aspect of CNS. It can effectively solve some traditional problems, such as hacker attacks, virus attacks, etc. There are many risk factors in practical application. For example, hackers steal user information, trojan horse programs invade hosts to steal confidential files, and there are loopholes and hidden dangers in the network system itself, which may lead to these hazards or cause serious consequences or even endanger CNS. Therefore, BD technology is an emerging technology with strong comprehensiveness and high value. As a new means of network security, BD technology is based on the transformation of traditional database model and various application systems on the Internet to improve its security. At present, there are a large number of massive information resources on the Internet. By analyzing these data, we can find many valuable and representative aspects that can provide users with better services. We can use the large number model to transform all the content that may be attacked or stolen in the network into a knowledge base that users need, so as to achieve the goal of computer security technology prevention and management. This paper studies the encryption algorithm based on BD. Assuming that there are many energy consumption combination forms pre (e,..., ea) that leak the unmasked intermediate combination value comb (C,,..., ca) information, the union of energy consumption sample positions they contain is t={..., t,}, n>d, and the energy consumption of the location set t on the energy trace p is extracted as the energy trace feature vector e=p [t], then Pr (e | comb) can be described by multivariate Gaussian distribution.

$$Pr\left(e\middle|comb_i\right)=\frac{e^{-\frac{1}{2}(e-\mu_i)^T\sum_i^{-1}(e-\mu_i)}}{\sqrt{(2\pi)^n\left|\sum_i\right|}} \tag{1}$$

Among them,

$$\sum_{\mathrm{i}} = \frac{1}{\left|S_{\mathrm{i}}\right| - 1} \sum_{e \in S_i} e, e \in S_i \tag{2}$$

In order to ensure the confidentiality, security and readability of user identities and passwords in different fields under the Internet environment, users can get the security resources they need better and faster. Therefore, we need to research and develop network encryption technology.

3. Experimental Process of CNS in the Background of BD

3.1 CNS Protection Framework Based on BD

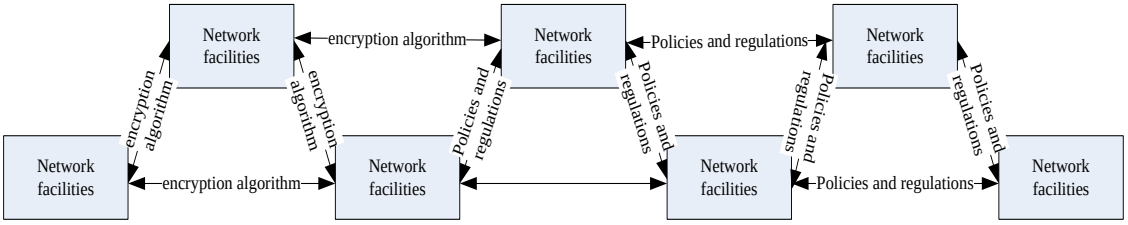

Figure 1: CNS Prevention Framework based on BD

In the process of CNS, people demand more and more information. From the current situation of CNS, the CNS protection system includes the collection, analysis and transmission of BD, as well as effective screening of massive information, and taking corresponding strategies according to different situations. In order to ensure that users can access Internet resources at any time without being stolen or deleted by individuals, and prevent illegal use of network equipment or hacker attacks, it is necessary to connect the server and the host into two independent systems in an overall network for isolation, so as to ensure the security of information transmission, the communication is not damaged, and the confidentiality is good. Therefore, in order to better cope with this change, many new problems have been brought about. A series of challenges, such as how to strengthen user privacy protection, how to effectively prevent hacker attacks, and also to improve their ability to resist virus intrusion and prevent system vulnerabilities, need further research and exploration to get faster, more effective and safe applications, so as to achieve the healthy growth of computer network technology, as shown in Figure 1.

3.2 BD Based CNS Performance Test

In the testing stage of CNS, we can analyze the data storage mode, access method and use authority according to different users. In the process of software growth, through the testing of the system, it is found that there are security risks, and it is necessary to modify and maintain them in a timely manner. The first is network attack detection. First, it is necessary to analyze whether the intruder has used computer technology or other improper means. Second, it is necessary to detect whether authorized users have access to network information resources and sent emails to obtain permissions. Finally, data files, hardware devices and important files are encrypted to prevent hackers or malicious programs from entering the system to steal relevant confidential information.

4. Experimental Analysis of CNS in the Background of BD

4.1 BD Technology Performance Test of CNS

Table 1 is the BD technical performance test data of CNS.

Table 1: Big data technology security performance test

Test times	Data segment	Intercepting data segments	Safety prevention rate(%)
1	321	319	94
2	341	340	97
3	325	322	90
4	366	364	99
5	315	313	93

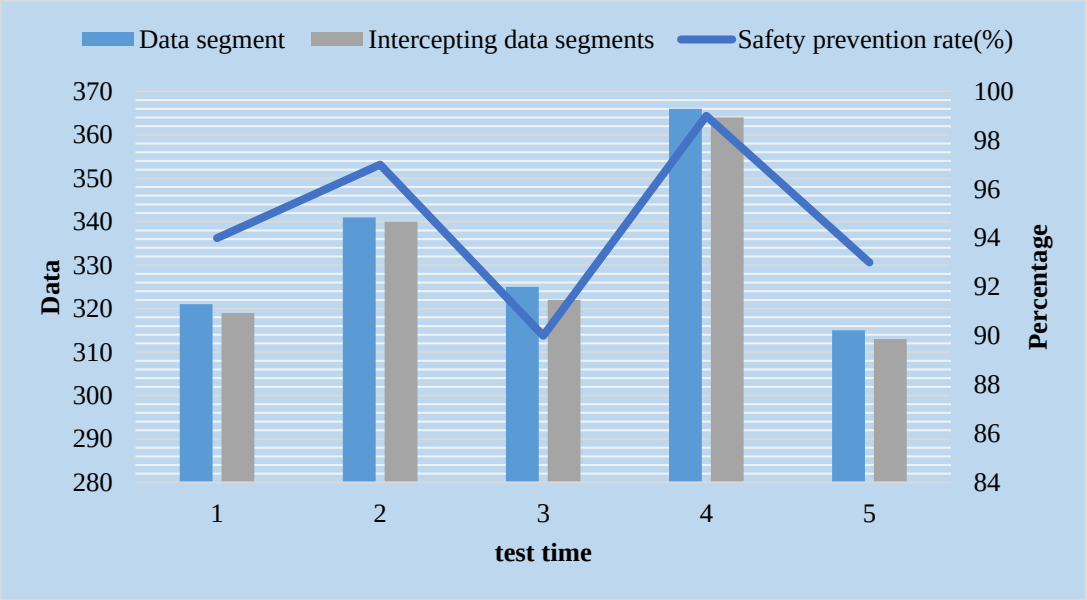

Figure 2: Big data security prevention performance

During the performance test of CNS technology, it is mainly to effectively control the data collection, storage and transmission. First of all, we should ensure that data information is not stolen illegally. Second, we should improve the encryption algorithm, key management and user authentication methods. Third, we should prevent hacker attacks or Trojan viruses from invading through firewalls. Finally, we need to strengthen the detection of the internal server environment of the large database management system to reduce the probability of potential network security risks, so as to ensure that the computer system can operate normally and has high performance value. It can be seen from Figure 2 that the security protection of BD based encryption algorithm for data is more than 90%, which indicates that the CNS requirements can meet the requirements.

5. Conclusions

In recent years, with the continuous growth of Internet technology, CNS issues have become increasingly prominent, posing a serious threat to people's lives and work. This paper analyzes and studies the CNS in China under the background of BD. This paper first expounds the concept, characteristics and current risk situation in the age of BD, and then proposes how to effectively prevent and control intrusion attacks in the cloud computing mode from the perspective of firewall and encryption mode, set up the identity recognition function and key management mechanism to prevent illegal elements from stealing information, and establish the corresponding database for emergencies.

References

[1] AbdAllah A. AlHabshy, Bashar I. Hameed, Kamal Abdelraouf Eldahshan: An Ameliorated Multiattack Network Anomaly Detection in Distributed Big Data System-Based Enhanced Stacking Multiple Binary Classifiers. IEEE Access 10: 52724-52743 (2022).

[2] Negin Alemazkoor, Mazdak Tootkaboni, Roshanak Nateghi, Arghavan Louhghalam: Smart-Meter Big Data for Load Forecasting: An Alternative Approach to Clustering. IEEE Access 10: 8377-8387 (2022).

[3] Turki Ali Alghamdi, Nadeem Javaid: A Survey of Preprocessing Methods Used for Analysis of Big Data Originated From Smart Grids. IEEE Access 10: 29149-29171 (2022).

[4] Hanan E. Alhazmi, Fathy E. Eassa, Suhelah M. Sandokji: Towards Big Data Security Framework by Leveraging Fragmentation and Blockchain Technology. IEEE Access 10: 10768-10782 (2022).

[5] Mohammad Bigdeli, Shahrokh Farahmand, Bahman Abolhassani, Ha H. Nguyen: Globally Optimal Resource Allocation and Time Scheduling in Downlink Cognitive CRAN Favoring Big Data Requests. IEEE Access 10: 27504-27521 (2022).

[6] Dina Fawzy, Sherin M. Moussa, Nagwa L. Badr: The Internet of Things and Architectures of Big Data Analytics: Challenges of Intersection at Different Domains. IEEE Access 10: 4969-4992 (2022).

[7] Ahmad B. A. Hassanat, Hasan N. Ali, Ahmad S. Tarawneh, Malek Q. Alrashidi, Mansoor Alghamdi, Ghada Awad Altarawneh, Mohammad Ali Abbadi:Magnetic Force Classifier: A Novel Method for Big Data Classification. IEEE Access 10: 12592-12606 (2022).

[8] Mohammed Arshad Khan, Mohd Shuaib Siddiqui, Mohammad Khalid Imam Rahmani, Shahid Husain: Investigation of Big Data Analytics for Sustainable Smart City Development: An Emerging Country. IEEE Access 10: 16028-16036 (2022).

[9] Pawel Kowalczyk, Mateusz Komorkiewicz, Pawel Skruch, Marcin Szelest: Efficient Characterization Method for Big Automotive Datasets Used for Perception System Development and Verification. IEEE Access 10: 12629-12643 (2022).

[10] David Chunhu Li, Michael Yu-Ching Lin, Li-Der Chou: Macroscopic Big Data Analysis and Prediction of Driving Behavior with an Adaptive Fuzzy Recurrent Neural Network on the Internet of Vehicles. IEEE Access 10: 47881-47895 (2022).

[11] Magda M. Madbouly, Saad M. Darwish, Noha A. Bagi, Mohamed A. Osman: Clustering Big Data Based on Distributed Fuzzy K-Medoids: An Application to Geospatial Informatics. IEEE Access 10: 20926-20936 (2022).

[12] Sooksan Panichpapiboon, Kavepol Khunsri: A Big Data Analysis on Urban Mobility: Case of Bangkok. IEEE Access 10: 44400-44412 (2022).