Design and Implementation of Network User Abnormal Behavior Detection System Based on Large Data Processing Technology

Zhu Hongjun[1], Gan Ruijie[2]

[1]Recruitment Office of Graduate School, Civil Aviation Flight University of China, Guanghan, Sichuan, China

[2]College of Computer Science and Technology, Civil Aviation Flight University of China, Guanghan, Sichuan, China

Keywords: Big Data, Network, User Abnormal Behavior, Design, Implementation.

Abstract: In the era of big data, network security has been attached great importance to by relevant industries, and network security problems still exist, mainly reflected in the increasing types of network attacks and the emergence of new attack modes, which has brought unprecedented threats to the operation of enterprise systems and is not conducive to the long-term development of enterprises. Based on this, through the analysis of large data processing technology, this paper innovatively designed a network user abnormal behavior detection system, and proposed specific implementation path.

1. Introduction

1.1 Literature review

The rapid development of big data technology has effectively improved the processing ability of massive data information. In view of the characteristics of the current big data processing technology, Ma Lixin et al. analyzed the methods of detecting users'abnormal behavior with the help of big data processing technology, which is conducive to ensuring network security (Ma et al,2018).Zhou Tao found that the current sustained network attacks have become one of the main threats to enterprise-level security users. By analyzing the current network abnormal behavior detection methods, and based on statistical learning method, the architecture of network abnormal behavior detection is designed, which is helpful for users to extract relevant parameters and obtain corresponding information, and lays a foundation for future research in related fields (Zhou,2015). In order to achieve better monitoring effect of abnormal network traffic, Yang Qing studied the monitoring method of abnormal network traffic in large data environment, which is helpful to improve the detection efficiency and accuracy of abnormal network traffic, ensure network security and create a good network environment for users (Yang,2018). Based on the existing large data platform, Zhang Xinzhao collects massive data information comprehensively, analyses data processing and application methods, and uses intelligent analysis engine and human-computer interaction analysis method to comprehensively detect and analyze network external attacks, which is conducive to the security, controllability and visibility of network information (Zhang,2018).

1.2 Purpose of research

With the rapid development of Internet industry, international data exchange is becoming more and more frequent. In the process of residents'life and enterprise operation, computer technology plays a vital role. Especially in recent years, the rise of big data technology has gradually brought human beings into the era of network information. In this era of big data, while the emerging Internet technology is widely used by human beings, the potential network security problems have also been highly valued by many industries. Moreover, in the increasingly complex network environment, network attacks tend to diversify and complicate gradually, constantly producing new means of attack, which brings adverse effects to the operation of enterprises, and even causes huge economic losses. In this context, the traditional abnormal behavior detection methods of network

Copyright © (2019) Francis Academic Press, UK DOI: 10.25236/scmc.2019.069

users have been unable to adapt to the new data analysis and processing capabilities, and the matching with the development of related industries has gradually decreased. Therefore, based on the background of large data, it is of great practical significance to study the abnormal behavior detection system of network users based on large data processing technology.

2. Analysis of Big Data Relevant Processing Technology

In the process of abnormal behavior detection of network users, there are many large data technologies involved. Therefore, before the design of abnormal behavior detection system for network users, the analysis of large data related processing technology is conducive to improving the application efficiency of related technologies.

2.1 Acquisition technology

As an efficient and safe data processing technology, data acquisition technology plays an important role in guaranteeing the data security of different systems (Yang et al,2018). Data collection technology is mainly to develop different types of data sources and some data sending purposes in the system, to ensure that the system can support different use protocols. At the same time, data acquisition technology can provide users with the corresponding raw data technology and retrieval function, and can also process some simple data, which is conducive to improving the user's data utilization efficiency. The implementation of data acquisition technology is small, which can enrich the functions of data acquisition, storage and forwarding. It is conducive to improving the management functions of related systems and improving the utilization efficiency of system data.

2.2 Distributed Technology

In related systems, distributed technology is a publish-subscribe system. The main reason is that after the system producer publishes a data to a user, the relevant participants subscribe to a queue. In this process, a large amount of data can be generated in the subscription queue, and the middleman can use distributed technology to send data to the majority of consumers. In the actual application process, distributed technology has the function of high throughput, can process hundreds of thousands or even tens of millions of information in one second, and effectively improve the data response rate.

2.3 Data Processing Technology

In the system, data processing technology occupies an important position. The data core components in the system adopt some commercial versions, through certain deployment and installation, to maximize the efficiency of optimal configuration in different components. With the help of data processing technology, the compatibility and stability of data can be greatly improved, and the efficiency of data use can also be improved. In the actual application process, data processing technology can greatly reduce the cost of data utilization, which is conducive to the efficient operation of related systems.

2.4 Data Warehouse Technology

Data warehouse technology is a new big data technology based on data processing technology. In the actual application process, in order to reduce the batch processing system of the related compilation work and maximize the avoidance of the defects of the related system, the relevant personnel all adopt data warehouse technology to store and use the system data (Zhang et al, 2016). In addition, considering the system, the relevant data may be separated, and some interest according to the task, the relevant personnel use data warehouse technology to process and analyze the off-line data. In addition, because the log data cannot be effectively changed under the background of no operation, and the existing search engines in the system cannot meet the search of relevant data, so the use of data warehouse technology can speed up the efficiency of data retrieval.

2.5 Real-time Data Processing Technology

In the system, real-time data processing technology is an effective way to implement data processing with the help of related components of data analysis. In the actual application process, data analysis needs to collect, screen and analyze massive data in large-scale systems to provide basic data application guarantee for users. In the specific application process, real-time data processing technology can support user interaction and iterative procedures, provide rich data resources, and help users extract relevant information. Therefore, in the process of system application, real-time data processing technology is very suitable for data ecosystem, which can provide users with a programmable system that can read, maintain and test, and break the problem of users writing massive data. Moreover, the user can improve the performance of the data system with the help of real-time data processing technology, which complements the process of data processing, analysis and calculation, and greatly improves the user's convenience.

3. Design of Network User Abnormal Behavior Detection System Based on Large Data Processing Technology

In recent years, with the continuous development of information technology, the problem of network information completeness has become increasingly prominent. The detection of abnormal behavior of network users in different industries has attracted wide attention from all walks of life. In this context, the task of anomalous behavior detection for network users in related industries is challenged. By combining with the rapid development of information technology, the related industries can build a network user abnormal behavior detection system, which can enhance the network user abnormal behavior awareness, accurately obtain the path of unsafe data attacks, and use intelligent methods to maximize the defense capability of the system, and fully protect user data security. To this end, based on the above data processing technology, this paper innovatively designs a network user anomaly detection system, as shown in Figure 1.

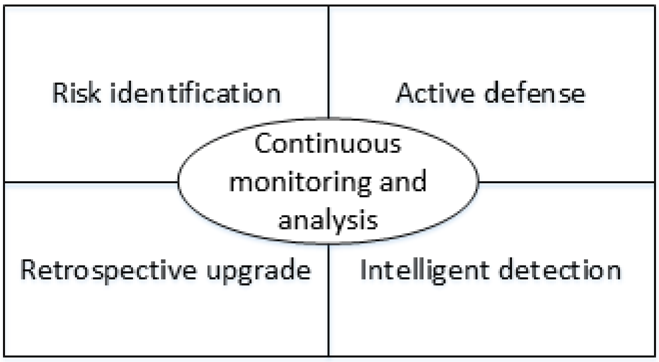

Figure 1. Network User Abnormal Behavior Detection System

In the network user abnormal behavior detection system, through the comprehensive analysis of enterprise internal information security management risk, combined with the current situation of security management system in different industries, and proceeding from the actual operation of enterprise business, an all-round behavior detection system is formed, which is conducive to ensuring the data security of enterprise system. . In the anomalous behavior detection system of network users, the core value of information security management is highlighted from three aspects: people, things and things. The anomalous behavior of network users is analyzed in detail, and then a capability matrix of anomalous behavior detection and management is formed. In the network user abnormal behavior detection system, a 360-user abnormal behavior detection technology system has been formed, which is conducive to the implementation of enterprise's defense ability against external bad information, and lays a good foundation for improving enterprise's security situational awareness ability.

On the basis of the network user abnormal behavior detection system, it can also evaluate the security performance of enterprise system comprehensively. Combining with the current situation of enterprise security management and based on the internal and external abnormal behavior, it can provide comprehensive and accurate risk data distribution for managers, and maximize the ability of enterprise system to defend the outside world. Now the ability to reflect internal and external security incidents, so as to achieve the effective management and control of the network users abnormal behavior detection system. In addition, in the anomalous behavior detection system of network users, through the establishment of adaptive risk management and control system, the system can effectively identify the risks and enhance the system's active identification and defense capabilities. Moreover, in the intelligent detection link, with the help of the network user abnormal behavior detection system, the enterprise can accelerate the application of some knowledge data, and form three aspects of detection procedures: before, after and in the event, which is conducive to improving the continuous defense and detection ability of the enterprise system.

4. Mplementation Path of Network User Abnormal Behavior Detection System Based on Large Data Processing Technology

4.1 Improving Information Management System

Perfect information management system is the basis of the implementation of abnormal behavior detection system for network users. For some large-scale projects, the demand of users and enterprises is relatively large, which contains a large amount of information data. This requires enterprises to have a sound information management system to support the effectiveness of the operation of related systems. On the basis of the original information management system, enterprises should sort out the information needed by business, identify and classify different information, and then store them separately according to different data volume to ensure the validity of relevant information in the system. In addition, enterprises should protect the security of abnormal behavior detection system of network users and information management system by standardizing the way related personnel access the information management system, with the help of some security protection software or systems.

4.2 Strengthen the System Detection

In order to ensure the effectiveness of the application of abnormal behavior detection system for network users, relevant departments should strengthen the detection of the system. In the detection of abnormal behavior detection system for network users, enterprises should give full play to the advantages of the current robot detection system, combine the manual detection method with the robot detection method, form a preventable dynamic detection mode, and carry out the detection work regularly or irregularly to ensure that network users are different. Effectiveness of Constant Behavior Detection System. The application of robot detection method can reduce the work intensity of manual detection to a certain extent, and can effectively reduce the detection error of abnormal behavior detection system for network users. Enterprises should combine robotic detection methods with manual assistant detection methods, through the detection of abnormal behavior detection system of network users, find out the hidden safety hazards in the process of system operation in time, and then ensure the safe and stable operation of abnormal behavior detection system of network users.

4.3 Establishment of Internal Operational Responsibility System

Enterprise insiders belong to the theme of abnormal behavior detection system of network users. Establishing the responsibility system of enterprise internal operation can provide basic guarantee for the operation of abnormal behavior detection system of network users, and it is also one of the ways to realize abnormal behavior detection system of network users. Enterprises should establish internal operation responsibility system to implement the relevant responsibility of abnormal behavior detection system for network users, and implement it to individuals to enhance the sense of responsibility of relevant personnel, which is conducive to building corporate culture and promoting the effectiveness of the application of abnormal behavior detection system for network users. Moreover, the establishment of internal responsibility system is conducive to promoting relevant personnel to adopt positive methods to ensure the safe and stable operation of abnormal behavior detection system for network users. At the same time, enterprises can also learn from some successful experience. In the process of implementing the abnormal behavior detection system for network users, some incentive mechanisms are introduced to encourage the relevant personnel to fulfill their personal responsibilities and fully mobilize the enthusiasm of the staff, which is conducive to the application of the abnormal behavior detection system for network users and has been in normal condition.

Acknowledgements

This research has been financed by the Natural Science Foundation of Civil Aviation Flight University of China in 2019, the application of data mining technology in the enrollment of graduate students in civil aviation colleges and universities (J2019-007) and the research on the training and selection mechanism of outstanding graduate students in our university (XKJ2018-14) in the subject construction fund project of Civil Aviation Flight University of China in 2018 .

References

[1] Ma L.X., Xu B., Li L.B., et al.(2018).Network Abnormal Behavior Analysis and Monitoring System Based on Big Data Technology, Communication Power Supply Technology,35(07):162-163.

[2] Zhou T.(2015). Network abnormal behavior detection technology based on statistical learning, Big data, 1(4):38-47.

[3] Yang Q.(2018).Abnormal network traffic detection based on large data analysis, Mechanical Design and Manufacturing Engineering,47(11):83-86.

[4] Zhang X.M.(2018).Research on Security Perception Strategy of Large Data Analysis Based on Network Operations and Maintenance, Network Security Technology and Applications,18(9):67,35.

[5] Yang Xi.S., Jiang L., Peng X., et al.(2018).Research on anomaly detection method based on large data,Computer Engineering and Science,40(07):38-44.

[6] Zhang G.L., Pu H.P., Yu Y.L.(2016).Research and Practice on Promoting Education Informatization Based on Big Data Technology: A Case Study of Southwest Petroleum University, Journal of Sichuan College of Arts and Sciences,26(2):125-130.