Research on Network Security Analysis Based on Big Data Technology Application

Qiang Zhang¹* and Dehui Ma¹
¹Shandong Yellow River Information Center, Jinan, Shandong, China, 250013

*Corresponding author e-mail: zhangqing@yrcc.gov.cn

Abstract. With the maturity and expand of big data tech, based on BDA, it can realize the real-time monitoring of network data and information, and help the system to make autonomous and dynamic decision-making and processing of network security events. At present, there are still some problems and deficiencies in the utilization of Network Security Analysis (NSA), which need to be improved urgently. Based on this, this paper first analyses the current situation of Computer Network Security (CNS), then studies the characteristics and utilization of big data tech, and finally gives the specific implementation and utilization of network security based on big data tech.

Keywords: Network Security, Big Data, Tech Utilization

1. Introduction
With the rapid expand and iteration of computer information tech, the related tech relying on computer big data has been widely used and developed in various industries. However, the deepening of the utilization of computer big data tech has brought opportunities for all kinds of illegal behaviors, especially various network attacks, network intrusion and information theft. It can be seen that the current network information security, whether it is the level of risk or the degree of threat, has reached a point that cannot be ignored[1]. The current network attacks facing the computer information network show the expand trend as shown in Figure 1.

![Figure 1. The expand trend of current network attacks.](image-url)
Under this expand background, only the comprehensive utilization of a variety of computer NSA tech can effectively deal with the occurrence of network security incidents. With the continuous progress of big data tech, the utilization of its advantages in data analysis and behavior research in network security incident analysis has a realistic foundation, and makes it possible to carry out (Network Security Analysis) NSA based on big data tech and take targeted measures and actions to protect network security. On the other hand, with the expand of computer network in various industries, a large amount of data and information are generated. How to safely and efficiently mine and utilize the practical value brought by these data and information has become one of the utilizations focuses of current computer big data tech. However, there are still some problems and deficiencies in the utilization of big data tech in NSA as shown in Table 1, which urgently needs to be improved.

Table 1. Status of big data tech in NSA utilization.

| Aspects          | Status                        | Problems and deficiencies                        |
|------------------|-------------------------------|--------------------------------------------------|
| Data analysis    | Focus on structured data     | Most of the data in the utilization is unstructured |
| Operating mechanism | Single department or business unit | The conclusion is one-sided                      |
| Data type        | Focus on transaction data    | Lack of analysis of operational data              |

Based on the continuous expand and improvement of the advantages of computer big data tech in the aspects of information analysis insight, information integration, data mining ability, etc., it has great utilization space and utilization prospect in network security\cite{2}. Based on BDA (BDA), it can realize real-time monitoring of network data and information, and help the system to make autonomous and dynamic decision-making and processing of network security events.

In addition, based on the advantages of computer BDA tech, network security information can be deeply mined and analyzed, so as to effectively carry out NSA and evaluation, and make rapid judgment and early warning for network security anomalies and security situation, and help network security responders to timely perceive the network security situation, so as to take countermeasures. Therefore, research on the utilization of big data tech in NSA has important practical value.

2. Analysis of the current situation of computer network security

2.1. Key issues of current computer network security

First, in the security level of website and system, it mainly includes malicious web page, malicious content, security vulnerability, website environment/security, attack risk, etc\cite{3}. Among them, security vulnerabilities include utilization vulnerability, web utilization vulnerability, operating system vulnerability, network device vulnerability, security product vulnerability and database vulnerability, while malicious web pages mainly include false release, malicious code, false shopping and website blackout. Secondly, in the key infrastructure safety level, it mainly includes the following aspects as shown in Table 2, namely, the people's livelihood, public service and basic production.

Table 2. Key infrastructure safety of computer network.

| Aspects         | Importance                        | Function                                                   |
|-----------------|-----------------------------------|------------------------------------------------------------|
| Public          | Related to the production and life | Normal operation of society                                |
| Livelihood      | Public service infrastructure      | Related to people's work and life                           |
| Basic production| Key production equipment           | Energy, transportation, TV broadcasting, data centre, etc  |
| Infrastructure  | Government dept, enterprises, institutions | Related to the normal operation of the social security. |

In addition, in the aspect of institutional data security, it mainly includes the data leakage involving the institution and the data leakage of third-party institutions\cite{4}. In the aspect of Internet of things
security, it mainly includes that malicious programs and their variants will destroy intelligent devices, cause data leakage, and lead to malicious attacks. When smart devices are associated with other devices, the security vulnerabilities of their own or connected devices are easy to be exploited and attacked. In the cloud security level, the network security problems mainly include privacy infringement, data loss, and confidentiality violations. Finally, the security level of artificial intelligence mainly includes several aspects as shown in Figure 2 below.

![Figure 2](image)

**Figure 2.** The security aspects of artificial intelligence.

2.2. Key contents of computer network security

The key content of computer network security mainly includes personal data and privacy protection, malicious programs, security vulnerabilities and the threat of illegal production. In the aspect of personal data and privacy protection, with the advent of big data era and information economy, the economic value of data is rising. Network attackers begin to obtain personal sensitive data through various channels and methods, and then cause data leakage[5]. Therefore, network security needs to focus on personal data and privacy protection. Secondly, at the level of malicious program, it mainly refers to stealing sensitive information of users through false and fraudulent bad information, hanging horses and malicious links or black chain and malicious hijacking.

In addition, in terms of security vulnerabilities, the main security vulnerabilities are personal utilization software and personal devices. The black industry threat is mainly to steal users' privacy, conduct illegal business activities, and threaten users' related security, such as illegal access to citizen information for precision marketing, so as to make profits. Therefore, it is necessary to plan and design from the top level of the system to protect users' privacy.

2.3. Current situation of network security market in China
With the continuous rise of emerging tech such as computer cloud computing, Internet of things and big data, the boundary between network data and information security is weakening, and the content of security protection is increasing. In this context, on the one hand, network data security, network information security and other aspects are facing great challenges; on the other hand, the expand potential and growth space of NSA market are facing great opportunities with the continuous attention of people on data security and privacy protection. At present, the scale of network security market keeps increasing, and the scale of domestic network security industry has maintained a double-digit growth rate for many years. It is estimated that the scale will reach 100 billion yuan in 2020, as shown in Figure 3 below.

In terms of laws and regulations, with the continuous improvement of the public's attention to network security, a number of laws and regulations related to network security have been promulgated in China. For example, in order to further regulate the Internet news gathering, editing, reprinting and dissemination of traditional news media, in order to standardize the whole process of Internet information content management and law enforcement, the Internet news information service management regulations, Internet information content management administrative law enforcement procedures provisions were promulgated, and the network information release process was standardized.

![Figure 3. The scale of network security market.](image)

3. Research on big data tech and utilization

3.1. Typical characteristics of big data
With the in-depth utilization of computer tech, a large number of data have been produced, in which unstructured data occupy a large scale and have been significantly increased. The heterogeneity and diversity of big data are in many different forms. A large number of irrelevant information can be used to predict future trends and patterns. In depth and complex analysis, real-time analysis rather than batch analysis of data input is carried out. The requirement of real-time data stream processing is the key to distinguish big data reference from traditional data warehouse tech and Bi tech. In addition, big data also has the characteristics of multiple data sources, multiple data types and strong data relevance. In this context, the key techs involved in big data include massive data storage tech, real-time data processing, data high-speed transmission, and search and data analysis.

3.2. Security threats of big data and relative tech
In the current computer network security environment, the security threats faced by big data information mainly include big data infrastructure security, big data storage security, privacy leakage, advanced persistent attacks against big data, data access security threats and other security threats. In
order to effectively deal with network security threats, it is necessary to effectively perceive the network security situation machine, so as to effectively preprocess the network information and extract the situation characteristics of network security, including situation assessment, situation prediction and situation display. These processes involve several typical tech so as to display the whole network security situation in real time and accurately, and detect potential and malicious attacks.

3.3. Security threats of big data and relative tech
The utilization of big data tech in NSA can significantly improve the efficiency of information data transmission, which is mainly based on improving data storage capacity and ensuring data validity. Secondly, the utilization of big data tech can further improve the NSA system, and improve the accuracy of network security system processing data from multiple angles. In addition, the utilization of big data tech in NSA can effectively improve the depth of NSA, avoid the risks left by traditional tech, and improve the depth of NSA.

4. Research on NSA based on big data tech

4.1. NSA based on big data tech
NSA based on big data tech mainly includes data collection, data storage and multiple data analysis. Among them, in the data acquisition level, including data extraction, conversion and loading. The distributed data acquisition system is used to optimize and improve the reliability and availability. At the level of NSA, including the storage and collation of original data based on data size and type. At the level of multiple data analysis, the utilization of big data tech can effectively improve the efficiency of data collection and analysis, enhance the depth and breadth of data retrieval, and realize the comprehensive protection of network security.

4.2. Implementation of NSA based on big data tech
First of all, collect the whole domain security data of the whole network security defense chain, store and organize it organically, and build a perfect security database. Secondly, based on the effective planning, modeling and algorithm implementation of network security, a large number of data are deeply mined to discover potential threats and risks, and timely early warning and detection are carried out. In addition, based on the distributed file storage system, the network information security file data is divided into multiple data blocks for data import and export. Finally, the network security database is updated in time based on the cloud server or upgrade package for the effective response and processing of BDA system.

4.3. Utilization of big data tech in network security
The specific utilization of big data tech in network security includes attack detection, network anomaly detection, network security situation awareness and network threat intelligence analysis, among which the utilization in network attack detection is mainly based on big data tech to realize deep correlation analysis of network security data and intelligent association of multiple types of security data. The utilization of network anomaly detection is mainly based on the network user behavior analysis of big data to improve the pertinence of network anomaly detection. In addition, the utilization of network security situation awareness is mainly to realize network security situation awareness by using big data tech storage, parallel computing and efficient query. Finally, the utilization in network threat intelligence analysis is based on the visibility of big data tech and the comprehensive control of the whole network risk and threat.

5. Conclusion
In summary, with the continuous progress of big data tech, the utilization of its advantages in data analysis and behavior research in network security incident analysis has a realistic foundation, and makes it possible to carry out NSA based on big data tech and take targeted measures and actions to
protect network security. This paper discusses the necessity and effectiveness of the utilization of big data tech in the current NSA by analyzing the status quo of network security issues, as well as the expand of big data and the advantages of big data tech. Then through the analysis of the role and specific utilization of big data tech in NSA, the feasibility of applying big data tech to NSA is verified.

References
[1] Cui Quanxiu, Liu Fang. When big data meets software defined networking: SDN for big data and big data for SDN [J]. IEEE Network, 2016, 30(1): 58-65.
[2] Guan Lei, Hu Guangjun, Wang Zhan. Research on network security situation awareness tech based on big data [J]. Information network security, 2016 (9): 45-50.
[3] Hameed S, Ali U. HADEC. Hadoop based live DDoS detection framework [J]. Eurasip Journal on Information Security, 2018(1): 11.
[4] Liu Yi, Liu Ke, Kong Jiankun. Research on LTE network planning based on big data mining [J]. Communication tech, 2015, 48 (2): 194-198.
[5] Song Peng, Ludanyue, Zhao yanping, et al. New progress in big data research in social networks [J]. Lantai world, 2017 (12): 63-67.
[6] Wang Lei, Wang Xidian, Cheng Nan. Intelligent wireless network optimization system based on big data tech [J]. Telecommunication science, 2015, 31 (12): 159-163.
[7] Yan Shengfeng. Solving routing and wavelength assignment problem based on heuristic algorithm [J]. Journal of Huazhong University of science and tech, 2016, 72(9): 122.