The Discussion on Computer Network Information Security and Law Based on Big Data Technology

Hongyuan Pan

Oxbridge College, Kunming University of Science and Technology, Kunming, China

panhy86@163.com

Keywords: Big data technology, Computer, Network information, Information security, Law

Abstract: With the science and technology advancement, computer networks have developed rapidly, and big data has gained more room for development. But at the meantime, it also increases the instability of the data. The security of computer networks cannot be effectively guaranteed, and security problems are prone to appear. This article discusses computer network information security issues in the big data era, expounds the characteristics and development trends of network security legislation, and points out the development direction of China's information network security legislation.

1. Introduction

With social economy rapid development, computer network information platform has become a tool for people to communicate and communicate. Especially with the support of big data technology, the use of computer network platform has been expanded, but it has also brought greater security [1]. In the context of big data, the types of computer network information security risks are more diverse, threatening the computer network information security platforms, and detrimental to people's personal safety and property safety. Under such an environmental background, it is of great practical significance to explore the computer network information security risks and countermeasures under the big data background [1].

2. Big data analysis model

2.1 Association rule analysis (Apriori)

Apriori (a priori, speculative) algorithm is widely used, and can be used to analyze consumer market prices and guess customer consumption habits; intrusion detection technology in the field of network security [1].

The Apriori algorithm uses a layer-by-layer search strategy, and at the meantime compresses the search space according to its properties. And its nature is that if an itemset is frequent, all its non-empty subsets must also be frequent itemsets. Its basic idea is to scan the set of things once to find out the frequent 1-itemset set L1, and then based on L1, generate all possible frequent 2-itemsets, that is, the candidate set C2, and then make the necessary cuts to C2 based on L1 Branch operation [2]. After the optimization of C2 is completed, scan the transaction set again to find the next frequent candidate set, and iterate until no more frequent set is found, as shown in Figure 1.

In practical applications, association rules are mainly applied to the association behavior of commodity purchases. For example, for a store, the association analysis of big data analysis can discover the purchase behavior between bread and milk, so that targeted promotions or appropriate promotion can be carried out. Adjust the placement of items in the mall. Therefore, correlation analysis is a particularly effective model for big data analysis, and it is more targeted.

  DOI: 10.25236/icceme.2024.015

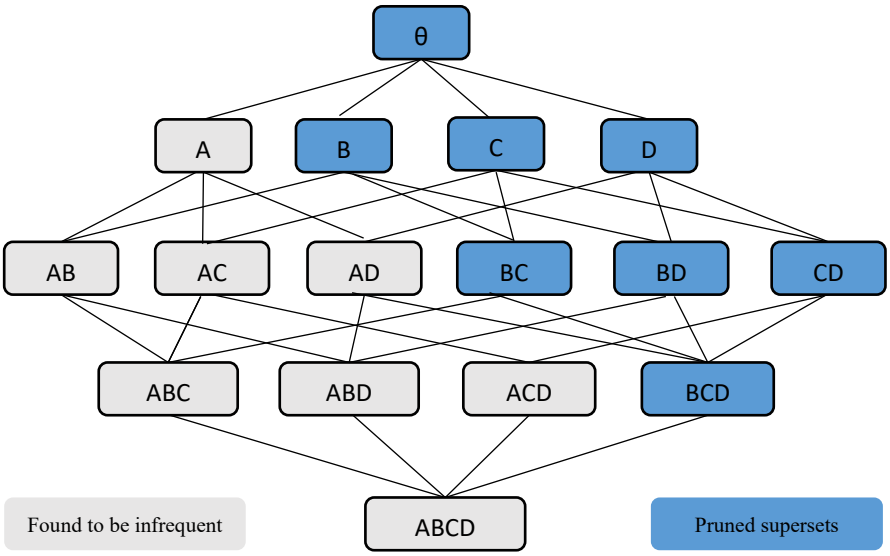

Fig.1 Association analysis big data analysis model

2.2 Cluster analysis model

The cluster analysis model refers to the dividing process, collection of physical or abstract objects into similar object sets. The result is that objects in the same cluster have higher similarity, while on between different clusters have higher similarities [2]. The three elements of cluster analysis are similarity measure, clustering criterion and clustering algorithm. The similarity measure is mainly used to measure the similarity of objects and the difference clusters, while the clustering criterion is used to evaluate the quality of the clustering results, and the clustering algorithm is used to find the extreme value of the criterion function the best clustering results [3]. The commonly used algorithms in big data clustering analysis mainly include partition clustering algorithm, density-based clustering algorithm, hierarchical clustering algorithm, and grid-based clustering algorithm. The more typical one is the partition clustering algorithm.

The representative of partition clustering algorithm is K-means algorithm, K-center point algorithm and some of their variants. The K-means clustering algorithm assumes that all data objects are divided into K clusters, the center of each cluster is represented by the mean, the similarity between objects is measured by distance, and the clustering criterion uses the error sum of squares criterion. Its core lies in first selecting K initial cluster centers and classifying each data object into each cluster according to the principle of minimum distance [3]. The cluster analysis model is a relatively simple big data analysis model, but it can efficiently divide large data sets. It is also the important data mining models and has been widely used in practical work.

3. The concept of network information security

Network security information refers to network information protection to prevent data leakage, modification or destruction caused by illegal use. Specifically, it refers to ensuring the information itself confidentiality and security in many fields' application such as computer, mathematics, and application communications. In the processing and protecting information process, ensure the information is complete and accurate. When the authorized person needs to consult various information, he can obtain information resources at any time [4], as shown in Figure 2. It is generally believed that network information security involves several aspects: First, the security status of Internet space, which includes maintaining Internet infrastructure and other equipment to ensure normal network operation. This primarily focuses on issues such as Trojan horse attacks, damage to hardware facilities, and difficulties in deciphering Internet passwords from a professional and technical perspective. Second, the reliability of network information content emphasizes controlling information leakage, harmful content, dishonest behavior, network hazards, and other related activities, highlighting the security challenges inherent in network transmission content itself [4].

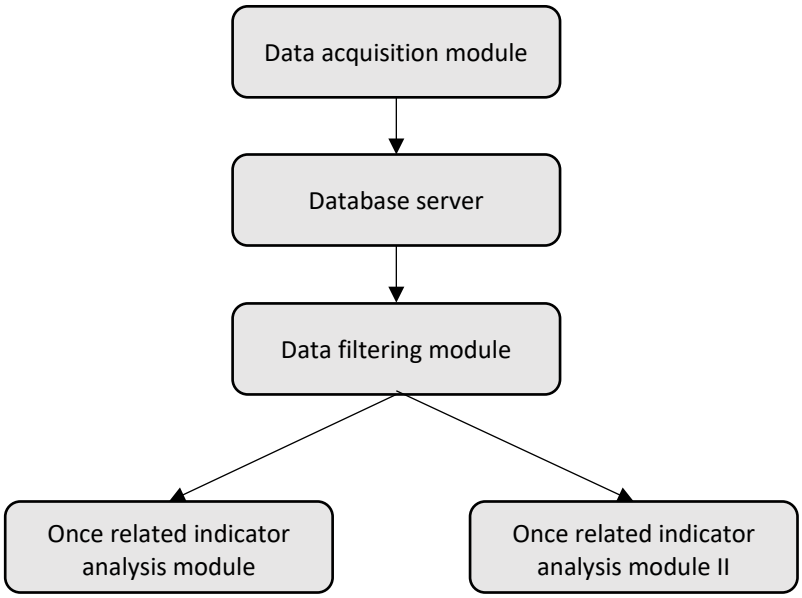

Fig.2 Network data security model

4. The network information security risks characteristics in the context of big data

In big data context, network information security mainly is concealment. The Internet virtual space has a wide range. Many participants are virtual characters, and their identities and roles have the characteristics of virtuality and concealment. When illegally stealing network information, they will not be restricted by space and time. Offenders can be at a certain time at will. Using hacker technology to steal network information, and the criminal process can be done without leaving traces, it is difficult to find and detect [5]. The second is intelligence. The network information security risks are extremely intelligent. This intelligence stems from the rich computer network expertise of illegal intruders. They use network vulnerabilities and system defects to use their own computer network knowledge and technology to various methods have launched attacks on network systems and electronic data, stealing or destroying network information, as shown in Figure 3. The third is suddenness. Computer viruses are latent and unpredictable, just like an unknown "time bomb" [5]. If it is not prevented, once it breaks out, it will instantly cause the collapse of the entire LAN network system; the fourth is the seriousness of the consequences. In the big data context, network information security risks are even more harmful. This is because in the context of big data, individuals rely heavily on data collection and data analysis [5]. Once data is leaked or tampered will cause serious losses.

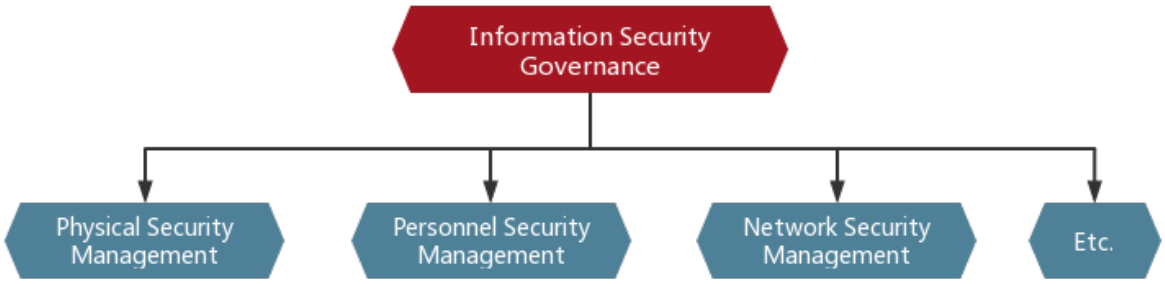

Fig. 3 Big data is used for network security management

5. Influencing factors of network information security

5.1 Inadequate relevant laws and regulations

In the face of increasingly arrogant and rampant cybercrimes, many countries have begun to draft laws and regulations on cyber information security [4]. It's just that cybercrime is different from real crime. Cybercrime is carried out with the help of a virtual platform such as the Internet, which makes it very difficult to collect evidence of cybercrime. At the meantime, the usual laws and regulations for traditional crimes cannot match the cyber information crimes. Until now, the boundaries of cybercrime are still very blurred. It is difficult for us to define cybercrime with a unified and clear boundary [1-3]. As a result, there are still many blanks that cannot be filled in the relevant laws and regulations of cybercrime, and the laws and regulations in the cyber world are not strict and clear enough.

5.2 Insufficient network information management system

The network information security management system occupies a very key position in network security, but in the consciousness and concepts of many relevant personnel, they often only attach great importance to technology and ignore the importance of management [4]. They hardly know that most information security problems are caused by management vulnerabilities. If the network information management system is not reasonable enough, there will be many hidden dangers in the security of network information, leaving opportunities for virus attacks and hacker intrusions, as shown in Figure 4. Relevant data shows that the negligence of the management system has caused about 80% of network information leakage [5].

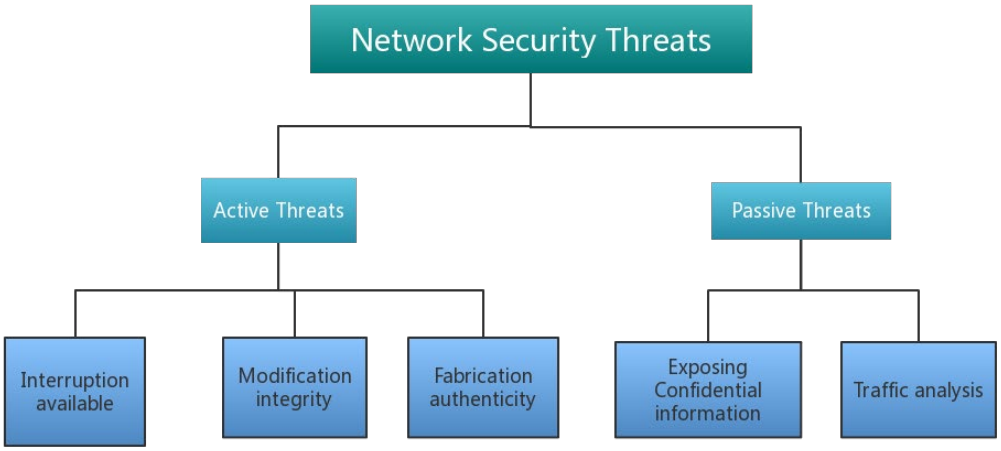

Fig.4 Hidden dangers of network information security

5.3 Network openness

The computer network itself has open characteristics, which is also a major advantage of computer network applications. However, this open characteristic also causes the computer network system to suffer from various network attacks. Once the security of computer network level is not high, or there are security vulnerabilities [2]. It will cause the distortion or theft of computer network information, and the openness of the network also creates the vulnerability of network security. Based on the open network environment, the network TCP/IP protocol cannot meet the computer network information security requirements under the big data technology, and the overall security is low [8]. In the operation of the security protocol, the network services and data functions cannot meet the user requirements [4].

5.4 Hacking

Hacker attacks are a common source of information security risks. This kind of man-made malicious attacks includes two aspects, as shown in Figure 5: One is active malicious attacks. After

the target is selected, the attack is carried out in a fixed destruction method, and the network security system is used. Vulnerability, stealing or destroying network system data, resulting in the lack of network information [2-4]. The second is to passively steal or crack the target information. The attack method has a certain degree of privacy and will not cause damage to the computer network system. Whether it is an active attack or a passive attack, it will have a big impact on the integrity of computer network information, threatening the security of computer network information, especially malicious attacks will also affect the use of computer network systems, causing system paralysis or delays, etc. problem [2].

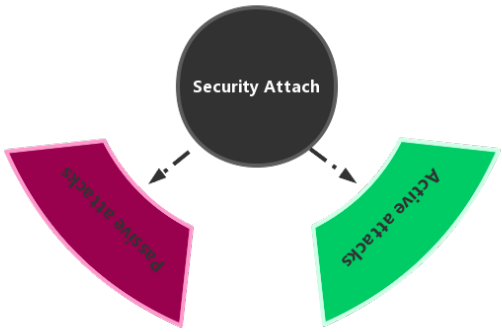

Fig.5 Attacks on information security

5.5 Human error

The safe operation information of the computer network system depends on the user's operating level, ability, and knowledge reserves. In the operation information of the computer network system, the possibility of human operation errors is prone to occur, causing computer network information security risks. In the context of big data, computer network information systems are used for data collection, sorting and analysis in various industries [1]. Due to insufficient user security awareness or lack of operating technology, user password settings and correct operations are likely to be inconsistent. It leads to the loss, tampering or leakage of computer network information, which constitutes a computer network information security risk.

5.6 Imperfect cyber security technology

The security of the network information system mainly includes four aspects: (1) the security of the host operating system layer; (2) the security of the application layer; (3) the security of the network protocol layer; (4) the security of the database management system layer.

The four security levels listed above still have security vulnerabilities to varying degrees. For example, at the level of network protocols, there are relatively large security vulnerabilities. In the information network system, the network protocol is its foundation. The Internet protocols we use today are generally the TCP/IP series. There are security flaws in the design of various application services and the communication process of the TCP/IP protocol family [5]. At the meantime, the method of transmitting data is in plaintext, so it will be subject to network attacks in the form of denial of service, data encoding, spoofing, and data interception. In addition, the current common operating systems such as UNUX or UNIX also have system security vulnerabilities in their own system design.

6. Strategies to strengthen information security of computer network and protection in the big data era

6.1 Protect the security of computer network information in accordance with the law

The scope of big data applications is very wide, and it has penetrated human work and life. With the science and technology continuous development, big data has gradually entered the era of intelligent information, which means that humans can obtain events in society at any place [3]. For

example, humans can use the technology of the big data era to understand the actual changing trends of logistics, the level of physical health and the status of the use of electrical equipment fully illustrate that the application of computer networks in the big data era provides many beneficial information for human life. Therefore, to effectively ensure the computer network information security, on the one hand, it is necessary to improve the relevant legal provisions for the information usage in the big data era, and on the other hand, it is necessary to formulate a special information security protection mechanism to reflect the authority and persuasive power of the law, and to ensure the integrity of computer network information [1-3]. In addition, relevant state agencies should strive to formulate effective security of network protection laws in the shortest possible time, so that people can ensure the personal information security during the use of computers.

6.2 Strengthen computer network information security management

In Internet industry has developed rapidly, and the authenticity of data information is also increasing, and it has multiple values. Therefore, more and more companies are developing computer technology and are committed to maximizing economic benefits, but they ignore the security of computer network information [5]. In response to this situation, and systematically manage and restrict computer-related companies. In addition, relevant agencies need to establish a professional management department for computer network information, and at the meantime require relevant personnel to regularly conduct anti-virus verification on the relevant code information of the network operation and use human inspection to ensure the security of the computer network system and ensure the network information security.

6.3 Pay attention to the application of security of computer network technology

To improve the computer network information security in the big data era, China needs to combine relevant laws and security technologies to further ensure the computer network information security. As relevant laws are still being improved, China needs to focus on the application of security of computer network technology, cultivate more network information security protection professionals, carry out computer network information security management in a realistic manner, and implement information security prevention work [4]. And then prevent hacker attacks and virus attacks, from the root to ensure the computer network information security.

7. Discussion on computer network information security legislation

At present, administrative legislation related to security management, administrative legislation related to the citizens' personal protection in electronic information, cybercrime legislation and related criminal procedure legislation [6]. The main characteristics are analyzed as follows:

7.1 Information network security protection law

The earliest released "Regulations on the Security Protection of Computer Information Systems" aimed at protecting computer systems and established a security protection system with security management and technical protection as the main body, such as the computer international networking filing system, the customs management system for computer information media, and computer security levels Protection system, computer room standards, etc., but there is no specific provision for violations of computer system security [6]. With the widespread use of the Internet and the increasing seriousness of network crimes, subsequent regulations such as the "Administrative Measures for the Security Protection of Computer Information Network International Networking" have expanded the scope of protection from computer systems to the entire computer information network and have stipulated more and more the more network violations and their administrative penalties [7].

To regulate the order of online social activities, China has promulgated the "Internet Information Service Management Measures", "Internet Electronic Announcement Service Management Regulations", "Internet Online Service Business Site Management Regulations" and other regulations and regulations and strengthened the management of network service providers. Strengthen network

security management and regulate network activities. These laws and regulations stipulate the obligations of network service providers to participate in network security management, including the obligation to prevent, report, and assist in investigations of network crimes [8].

7.2 Law on the protection of citizens' personal electronic information

China has not established a unified personal data protection law. The protection of citizens' personal information is decentralized in the Telecommunications Regulations, the Decision on Maintaining Internet Security, the Insurance Law, and the Law on the Prevention and Control of Infectious Diseases. "Postal Law", "Passport Law", "Practicing Physician Law", "ID Card Law" [9].

8. The Trend of Computer Network Information Security Legislation

With the network technology continuous development, as well as the impact of emergencies (such as the data breach of the U.S. Bureau of Personnel, Prism Gate, Ctrip downtime, Alipay disconnection), the legislation in the cyber security field in various countries is showing a trend of concentrated outbreak [10].

Facing the increasingly severe and complex domestic and international cyber security situation, major countries, and regions to cyber security legislation. Data protection provide a legal basis for the specific implementation of various cyber security protection measures [11].

At present, China's "National Cyber Security Law" (draft) has been officially released as the most effective law in the field of China's cyber security. In the future, with the implementation of the National Cyber Security Law, China's cyber security will surely usher in a new development situation. There will be laws to follow for cyber security assurance work, and violations of cyber security laws and regulations will also be severely punished [11]. As the number one brand in China's cyber security management, Newton Net Security must lead by example and be down-to-earth, assume the social responsibility of maintaining cyber security, and contribute its own strength.

9. Summary

To sum up, in today's era of data and information explosion and computer technology rapid development of, we are also always facing network information security risks. It analyze the sources and characteristics of computer network information security risks to prevent the occurrence of various security risks. Regulating cybersecurity practices, to continue to promote the legalization of China's cyberspace development process and implement top-level design, on the one hand, it is urgent to effectively sort out the relationship between basic laws and current laws and regulations and begin the formulation and adjustment of departmental and local legislation and policies. On the other hand, there is an urgent need to introduce a series of supporting regulations, including not only the formulation of lower-level laws such as the Measures for the Security Protection of Critical Information Infrastructure, but also more detailed regulations, industry-specific cybersecurity plans, and cybersecurity. Standard system, etc., to achieve effective convergence with basic laws.

References

[1] M. L. Sun, Research on China's Network Information Security Governance from the Perspective of Risk Society, *Nanjing Normal University*, vol. 44, pp. 132-135, 2019.

[2] M. Sh. Tang, On the Research of Security of computer network and Construction, *Digital Technology and Application*, vol. 32 (10), pp. 159-162, 2012.

[3] D.P. Wang, Research on Security of computer network and Prevention Strategy, *Science and Technology Vision*, vol. 26), pp. 226-227, 2012.

[4] G. Tian and X. H. Chen, Research on Security of computer network and Prevention Strategy, *Computer CD Software and Application*, vol. 23(03), pp. 100-103,2012.

[5] J. Y. Wen, Research on Security of computer network in the Big Data Era, *Computer Knowledge and Technology*, vol. 12, pp. 321-325, 2017.

[6] L. Ma, The legislative positioning, legislative framework and system design of the Cybersecurity Law, *China New Communications*, vol. 15, pp. 225-227, 2017.

[7] Ch. Zhang, Current Status and Trends of China's Cybersecurity Protection Legislation, *Southwest University of Political Science and Law*, vol. 21(14), pp. 321-324, 2018.

[8] L. X. Zhang, Analysis of Network Information Security Status and Information Security Countermeasures, *Nanjing University of Posts and Telecommunications*, vol. 13(11), pp. 215-217, 2017.

[9] F. Liang, Discussion on the Rule of Law for Network Information Security, *Network Security Technology and Application*, vol. 9(04), pp. 85-87, 2020.

[10] D. F. Wang and J. J. Li, Thoughts on Network Security Legislation Mode under the Background of Economic Globalization, *Wireless Internet Technology*, vol. 12, pp. 40-42, 2015.

[11] H. N. Ren, Development Process and Prospects of China's Information Network Security Legislation, *Network Security Technology and Application*, vol. 11(12), pp. 213-216, 2018.