Strategies Research on Computer E-commerce Security under the Background of Big Data

Wang Wenjuan

College of Arts and Information Engineering, Dalian Polytechnic University, Dalian City, Liaoning Province, 116600, China

Keywords: E-commerce security, Big data, Cloud computer

Abstract: With the rapid development of Internet and information technology, e-commerce has ushered in another wave of development. E-commerce facilitates people's life and shopping, but also brings a lot of security issues, such as issues of network security, privacy security and credit security. In order to solve these problems, this paper gives the security strategies of computer e-commerce in the context of big data, including intelligent firewall technology, data encryption technology, information recognition technology and illegal intrusion detection technology, to provide some references for the relevant researchers.

1. Introduction

With the rapid development of internet technology, the number of network users in China ranks first in the world [1]. The popularization and application of network is a prerequisite for the development of electronic commerce. With the huge number of network users in China, the development trend of e-commerce has become a new business model legend. The rapid development of e-commerce cannot be separated from the support of network technology. The number of Internet users in China and the expansion of e-commerce enterprises in recent years have led to the explosive growth of data storage in e-commerce enterprises. A large number of effective or ineffective shopping behavior leads to the generation of massive data, and the new development mode of e-commerce enterprises, such as directional advertising push, requires large capacity data processing capabilities to adapt to it. The development of e-commerce is accompanied by a variety of data. The faster the development of e-commerce, the larger the data scale. Big data refers to data with data volume above PB level. These data often carry a large amount of customer information and consumer information. E-commerce enterprises that have and are good at mining these data will often get new directions and momentum for development. At the same time, e-commerce platform gathers a large number of customer information and purchase information. If such information is leaked or stolen by illegal elements, it will cause great losses to customers. Big data technology can find abnormal points in the complex and changeable behavior of various transactions, and take the initiative to defend by capturing and comparing the abnormal points. We will reduce the transaction risk and form a more secure e-commerce transaction system. E-commerce has good prospects for development, but e-commerce enterprises are facing opportunities and opportunities in the era of big data, as well as challenges in data processing capabilities and data security protection [2].

2. Challenges of E-commerce Security under the Background of Big Data

2.1 Internet Security Problem

When consumers use e-commerce to conduct transactions, a large amount of data is exposed to the network, which provides hackers and computer viruses with the opportunity to invade. There are two kinds of intrusion. User intrusion refers to the use of system vulnerabilities for unauthorized access or higher-level permissions. Software intrusion, including virus worms, steals important information from computers. Denial of service attack is a destructive attack, which takes up a large amount of

  DOI: 10.25236/eeems.2018.036

network resources through legitimate requests and software vulnerabilities, increases the load of the server system, and causes the server to have no residual resources to provide services for other applications. And denial of service has relatively low technical requirements for the destroyer, so this attack is relatively simple to implement. But because its target is the server. In the era of big data, the consequences of server paralysis are quite serious. It refuses normal access to all users, and it is very likely to cause the paralysis of the whole system. Although the security of communication channel has always been a difficult problem, computer technology is also seeking different innovations and mass information transmission, which brings new pressures and challenges to transmission channel, such as channel security from information source to intermediary, information transmission between intermediary agencies, and channel security between intermediary agencies and consumer browsers. To ensure that the information can be sent to the correct recipient accurately, completely, timely and effectively, how to ensure the non-repudiation of the identity of the sender and the recipient, whether the information has been tampered with by interference, whether interception and eavesdropping, and whether it is abnormal interruption. These are all problems that need to be solved in the era of big data. Because virtualized data resources are distributed on the same physical resources, it is convenient for malicious users to implement channel attacks by means of shared resources [3].

2.2 Privacy Security Problem

In the traditional consumption mode, buyers and sellers conduct face-to-face transactions, so sellers generally do not require consumers to provide contact information, family address and other personal information with a certain degree of privacy [4]. However, in the consumption mode of e-commerce, these are often and must be filled in. Personal information is not only the basic information of these users, the bank account used in the process of payment, payment password and other information related to property, but also the various activities of users in the network, including users' recent browsing information in various websites, collecting goods of interest, etc. In an open network, even personal information stored on a computer hard disk or in a virtual space may be leaked. Because e-commerce operates on the Internet, the security level of the database of e-commerce enterprises is not very high, and the backstage access restrictions are not strict enough, resulting in the lack of effective protection of users' privacy information. Technical hackers are also more likely to invade. The illegal application of these users' personal information by e-commerce practitioners is also more convenient. The openness of data is one of the important characteristics of big data, which carries a large amount of privacy information of customers. In the information age, every data and byte in the computer is the flesh of privacy. In the era of big data, these data are also important factors to realize personalized services and precise push services, but openness inevitably involves the security and privacy of user data. They can store, analyze and even sell the user's personal information without the user's knowledge. The existence of these problems is an open secret in the industry. Users with ulterior motives can buy a large amount of user information at a small cost.

2.3 Credit Security Problem

Credit rating of both parties is the basic index to decide whether the two parties are trading or not. Compared with European and American countries, China still lacks mature credit mechanism to support the development of e-commerce. In the era of e-commerce, both sides of the transaction have the vitality. It is difficult to confirm the identity and credit rating of both sides of the transaction. Fake identity cheating users for money and transaction denial are also common in recent years. In this case, we urgently need to use big data technology to establish credit rating and identity recognition mechanism for each user online, so as to gradually improve China's e-commerce environment. Because the transaction in e-commerce is not face-to-face communication and negotiation between the two parties, neither party can see the other party's products to obtain more information. Only when the information provided by both parties is true and reliable, and there is no false deception, can the transaction be carried out smoothly. However, there are some people who have bad intentions. They pretend to be merchants on the Internet, compile their own relevant information at will, and use some false information to communicate with other users, thus cheating the trust of the other side to

reach a transaction, which seriously damages the interests of the other side. In reality, malicious breaches of computer network security have caused people's panic and anxiety about the security of computer electronic commerce. Computer e-commerce behavior has a series of attributes of commerce, but it is different from traditional commerce in operation environment, operation technology, operation means, operation mode and so on. This difference also puts forward special requirements for the security of computer electronic commerce under big data.

3. Strategies of E-commerce Security under the Background of Big Data

3.1 Intelligent Firewall Technology

Intelligent firewall refers to the correct judgment of programs with viruses, and then use decision-making, memory and statistics to identify and process data. Intelligent firewalls generally do not ask users, only when network access is uncertain, will the information be transmitted to users, and then invite users to take precautions together. Intelligent firewall can solve the problems of virus propagation, common denial of server attack and advanced application intrusion. However, compared with traditional firewalls, not every access program needs to ask users, so as to avoid frequent firewall alarm inquiries, making it difficult for users to judge by themselves. In view of computer virus damage, the application of firewall technology is a reliable barrier to the security environment of e-commerce. Big data is gradually changing people's way of life and expanding people's scope of life. Through the mining of big data, we can know customers better than customers. In view of customer’s consumption habits and consumption needs, more diversified products are produced to provide customers with personalized and humanized services, constantly improve and improve the service system of enterprises, so as to make services more optimized, products more excellent and customers more satisfied. Continuously improve the user experience, get consumer psychological dependence, get users' trust to make it become their loyal customers, and ultimately make it become the core competitiveness of enterprises. Using firewall technology, we can detect and identify data packets in e-commerce, shield illegal anomalous access, prevent virus programs from spreading to e-commerce platform, and protect the business platform and network environment. For the long-term development of e-commerce, building an independent network system and using firewall technology in LAN environment can ensure that e-commerce is more secure and reliable.

3.2 Data Encryption Technology

Although the application of firewall technology can play a certain security preventive effect, but its role is not completely safe, for some of the unsafe information that can bypass the firewall can do nothing. At this time, data encryption technology must be added to ensure the safety and reliability of data information. Data encryption technology can encrypt and protect all data information generated by e-commerce. It is difficult for illegal elements to steal personal information in high-intensity data encryption technology environment. Therefore, data encryption technology provides a green umbrella for e-commerce platform and network environment, so that user information and e-commerce information security can be disseminated. At present, most of them use programs or tools to encrypt files, such as file compression and encryption. Users can set personal passwords in the process of data compression. When decompressing files, they need to provide passwords to open files. Data encryption technology refers to the conversion of an information into meaningless ciphertext through encryption keys and encryption functions, while the receiver restores the ciphertext to plaintext through decryption keys to user important information such as password, identity card number, bank account, etc. In order to improve security, we can use data encryption technology to transform data information into meaningless ciphertext after encryption, prevent hackers from attacking, and improve the security of information systems and data.

3.3 Information Recognition Technology

In view of the unsafe problems caused by counterfeiting in the process of e-commerce transactions,

e-commerce management departments can use information identification technology to identify and verify counterfeiting, so as to ensure the authenticity and reliability of the identity of both sides of the transaction and the security of the transaction. Information recognition technology is a comprehensive anti-counterfeiting technology. It uses digital signature technology and identity authentication technology to convert personal information, trading habits, exchange information and so on, so as to form unrecognizable encrypted information, and cooperate with diversified personal authentication technology to make the identity of both sides of the transaction true. For example, CA digital certificate refers to an authoritative electronic document that can verify the identity of both parties in Internet e-commerce activities. Installing CA certificates on the server side of e-commerce platform can prevent counterfeiting websites, and installing CA certificates on the client side can be used to verify user identity and electronic signature. We can use information recognition technology to check whether the data provided by the other party is accurate and reliable, and further enhance the security of transactions. Digital signature mainly refers to the use of some digits to replace some important information in the exchange of information between the two parties, which can be known only after specific decoding, thus further improving the security of information transmission. Authentication is to check the basic parameters of the object to see whether it is true and effective, so as to further improve the security performance of e-commerce.

3.4 Illegal Intrusion Detection Technology

In the process of electronic commerce security prevention, the cooperation of illegal intrusion detection technology and firewall technology provides higher security. Illegal intrusion detection technology and firewall belong to two areas to prevent, the former against internal attacks, the latter against external virus attacks. Moreover, the former can detect and protect any unauthorized anomalous operations. Even if the firewall is bypassed and cannot be detected and eliminated, the anomalous access operations will be found through high frequency information analysis at key points by illegal intrusion detection technology, thus eliminating them. Therefore, the illegal intrusion detection technology and firewall construct two security barriers, the internal and external two layers of monitoring e-commerce activities, so as to ensure that the e-commerce environment is protected by two layers, equivalent to two security locks, greatly improving the security of e-commerce network environment and computer system. Intrusion detection is a technology to identify and deal with malicious use of computer and network resources. It can prevent unauthorized access or abnormal phenomena through in-depth detection of network groupings. Although firewall is an effective way to resist hacker access and virus intrusion, it is impossible for firewall to intercept all intrusions. This technology can detect viruses or hackers in time to prevent the invasion as soon as possible.

4. Conclusion

In the current society, the rapid development of computer technology has rapidly promoted the development of related enterprises. E-commerce is gradually established in the development of computer network technology, and has been more and more widely used in today's society. Solving the problem of network security and promoting the development of network security technology play an important role in the healthy and safe development of e-commerce. Therefore, we should apply scientific and reasonable network security technology, so as to promote the development of e-commerce better and faster.

References

[1] Gao Congshuo, Zang Chunling, Lin Chaoying. Research on the E-commerce Security and Development Trendsunder the Era of Big Data [J]. Innovation Science and Technology, 2016(6): 61-62.

[2] Liu Jing. The Practice and Development of E-commerce Platform in the Era of Big Data—A Case Study of Taobao [J]. Reformation & Strategy, 2016, 32(5): 122-126.

[3] Ye Min, Xie Qiyan. Discussion on E-commerce Security Problem Based on Computer Internet [J]. Value Engineering, 2016(31): 204-205.

[4] Deng Yi. The Application of Computer Network Security Technology in E-commerce [J]. China Computer & Communication, 2017(4): 194-195.