Journal of Economics and Public Finance
ISSN 2377-1038 (Print) ISSN 2377-1046 (Online)
Vol. 10, No. 2, 2024
www.scholink.org/ojs/index.php/jepf

Original Paper

Effective Application of Computer Network Security Technology in E-commerce Operation and Maintenance

Hongzhi Huang

School of Computer and Software Engineering, Xihua University, Chengdu, Sichuan 610039, China

Abstract

As an important part of the modern economy, the security of e-commerce operation and maintenance directly affects the business continuity of enterprises and the trust of users. This paper explores the application of computer network security technology in operation and maintenance, analyzes existing technologies and actual cases, evaluates its effects, and looks forward to future development trends. The paper shows that the use of advanced network security technology can significantly improve the security and reliability of e-commerce systems.

Introduction

It has developed rapidly around the world and has become an important way for people to shop and for enterprises to operate e-commerce. However, the booming development of e-commerce also inevitably brings serious security threats, including data leakage, hacker attacks, and malware. In order to ensure the normal operation of e-commerce systems and the security of user data, the application of computer network security technology is extremely important. This paper aims to systematically explore the actual application effects of these technologies in e-commerce and provide reference for future research and practice.

Keywords

E-commerce operation, Computer network security technology, Security of user data, Operation and maintenance, E-commerce business

1. Overview of Operation and Maintenance

1.1 Definition and Classification of E-commerce

E-commerce (E-commerce) refers to commercial activities of commodity transactions and service provision through the Internet. It uses Internet technology to digitize and network various computers in traditional commercial activities, thereby achieving a more efficient and convenient transaction process. E-commerce not only includes online commodity sales, but also involves online services, digital product sales, and electronic payments.

According to the different transaction subjects, e-commerce can be divided into the following main types:

- B2B (Business to Business): B2B e-commerce refers to the transaction of goods or services between enterprises through the Internet. This type of e-commerce usually involves wholesale business, with larger transaction amounts and lower transaction frequency, but the value of a single transaction is high. Typical representatives of B2B e-commerce include Alibaba, Made in China, etc.
- B2C (Business to Consumer): B2C e-commerce refers to the sale of goods or services by enterprises directly to consumers through the Internet. This is the most common form of e-commerce, where consumers can purchase a variety of goods and services through the enterprise's online platform. B2C platforms include Amazon, Tmall, JD.com, etc.
- C2C (Consumer to Consumer): C2C e-commerce refers to the transaction of goods or services between consumers through the Internet. The platform develops to provide trading platforms and payment services for individual sellers and buyers. Typical representatives of C2C platforms are eBay and Taobao.
- B2G (Business to Government): B2G e-commerce refers to the transaction form in which enterprises provide goods or services to the government. This type of e-commerce usually involves government procurement, public projects and bidding activities. Procurement information is released through the government electronic platform, and enterprises participate in bidding and transactions through the platform.
- C2B (Consumer to Business): C2B e-commerce refers to a form of transaction in which consumers provide goods or services to enterprises through the Internet. This model usually appears in the demand for customized goods or services, such as consumers post their needs on the platform, and enterprises provide customized products or services based on the needs.

In the process of e-commerce transportation maintenance, many types have their own unique needs and challenges. For example, B2B e-commerce needs to handle a large number of batch orders and emphasizes supply chain management and customer relationship management; B2C e-commerce needs to focus on user experience, logistics warehousing and after-sales service; C2C e-commerce needs to provide a safe and reliable trading platform and payment system to ensure the transaction security of individual sellers and buyers.

In actual transportation, these different types of e-commerce models need to adopt different technologies and management methods according to their specific needs and challenges to ensure the efficient and stable operation of the e-commerce platform.

1.2 Key Links in E-commerce Operation and Maintenance

Operation and maintenance is an important task to ensure the stable operation of e-commerce platforms and the quality experience of users. Operation and maintenance work involves multiple key links, including server management, database maintenance, network monitoring, website optimization and user support. These links together constitute the core content of e-commerce operation and maintenance.

Server management: The server is the infrastructure of the e-commerce platform, responsible for processing user requests, storing data and running applications. Server management includes server configuration, maintenance, monitoring and fault handling. In order to ensure the high reliability and availability of the e-commerce platform, operation and maintenance personnel need to regularly check server performance, update and maintain hardware and software in a timely manner, handle server failures and ensure the effective operation of data backup mechanisms and recovery.

Database maintenance: The database is the core component of the e-commerce storage platform data, including user information, product information, order information and transaction records. Database maintenance work includes database design, optimization, backup, recovery and security management. Operation and maintenance personnel need to regularly optimize database performance to ensure query speed and data storage efficiency. In addition, the improvement of database backup and recovery mechanisms can quickly restore data and ensure business continuity when data is lost or damaged.

Network monitoring: The network is the bridge between the e-commerce platform and user communication, and its performance and stability monitoring directly affect the user experience. Network work includes real-time monitoring of network traffic, detecting network delays and failures, analyzing network performance, and optimizing network configuration. Through network monitoring, operation and maintenance personnel can promptly discover and handle network problems to ensure the speed and stability of user access to the platform.

Website optimization: Website optimization is an active work to improve the user experience of the e-commerce platform, including page loading speed optimization, SEO optimization, user experience design optimization, and mobile terminal optimization. Through website optimization, operation and maintenance personnel can improve the access speed, search engine optimization, and user experience of the platform, thereby increasing user visits and transaction volume.

User support: User support is an important part of operation and maintenance work and is directly related to user satisfaction and loyalty. User support work includes online customer service, technical support, problem feedback, and after-sales service. Operation and maintenance personnel need to respond to user inquiries and problems in a timely manner, provide professional technical support and solutions, and ensure user satisfaction during the use of the platform.

Security management: With the increase in network attacks and data leaks, the security management of e-commerce platforms has become increasingly important. Security management work includes firewall configuration, intrusion detection, data encryption, vulnerability repair, and security audits. By strengthening security management, operation and maintenance personnel can effectively defend and respond to various network attacks and security threats, and protect user data and platform security.

Performance monitoring and optimization: The performance of the e-commerce platform directly affects user experience and business revenue. Performance monitoring and optimization work includes monitoring the platform's access speed, response time, transaction processing capabilities, etc., analyzing performance bottlenecks and optimizing them. Operation and maintenance personnel need to use performance monitoring tools to understand the performance status of the platform in real time, discover and solve performance problems in a timely manner, and ensure the efficient operation of the platform.

Through the community management and optimization of each key link, e-commerce operation and maintenance work can effectively ensure the stability of the platform, user security and experience, and provide solid technical support for the development of the company's e-commerce business.

1.3 Common Problems and Challenges in Operation and Maintenance

In the process of e-commerce operation and maintenance, common problems and challenges mainly include server downtime, network failure, database failure and security vulnerabilities. If these problems are not handled properly, they may lead to user data leakage, business interruption and damage to brand reputation.

Server downtime: Server downtime refers to the interruption of platform services due to hardware failure, software problems or failure to operate normally. Server downtime will not only affect the user's access and transaction experience, but may also lead to other loss of orders and business data. To prevent server downtime, operation and maintenance personnel need to establish equipment monitoring and fault handling mechanisms, timely discover and repair hardware and software problems, and ensure the high availability of the server. In addition, simulation configuration and load balancing should be implemented to improve the fault tolerance of the system.

Network delay: Network delay refers to the long time it takes for data to be transmitted in the network experience, resulting in slower user access to the platform. Network delay will significantly affect users and increase the user's loss rate. The causes of network delay may include network congestion, bandwidth operation and maintenance personnel need to optimize network configuration, increase bandwidth and transmission speed, and use content distribution networks (CDN) to accelerate data transmission. In addition, server architecture should be adopted to reduce the bandwidth physical distance between users and servers, thereby reducing network delay.

Database failure: Database failure refers to the inaccessibility or loss of data caused by hardware failure, software problems or operational errors in the database. Database failure will directly affect user transactions and data storage, resulting in business interruption and data loss. To prevent database failure, maintenance personnel need to regularly back up the database to ensure data security and recoverability. In addition, database performance should be optimized and high-availability architectures, such as master-slave replication and global databases, should be adopted to improve database reliability.

Security vulnerabilities: Security vulnerabilities refer to defects or loopholes in the system or software that can be exploited by attackers. Security vulnerabilities may lead to data leakage, system crashes and malicious attacks, posing huge security risks to e-commerce platforms. Operation and maintenance personnel need to regularly perform security vulnerability scans and patch updates to promptly repair known security vulnerabilities. In addition, multi-level security protection measures, such as firewalls, intrusion detection systems (IDS) and data encryption, should be adopted to improve the overall security of the system.

User data leakage: User data leakage refers to the unauthorized access, acquisition or use of user information, which may lead to user privacy leakage and property loss. Operation and maintenance personnel need to strictly control data access rights to ensure that only authorized personnel can access sensitive data. In addition, sensitive data should be encrypted for storage and transmission to prevent data leakage during transmission.

Business interruption and damage to brand reputation: Business interruption refers to the inability of e-commerce platforms to operate normally due to various failures or attacks, resulting in users being unable to access or use platform services. Business interruption will not only directly affect the company's revenue, but also damage brand reputation. To prevent business interruption, operation and maintenance personnel need to establish a comprehensive disaster recovery system to ensure that the system can be quickly restored in the event of a failure. In addition, an effective accident response mechanism should be established to handle emergencies in a timely manner and reduce the impact on users and business.

2. Overview of Computer Network Security Technology

2.1 Basic Concepts and Classification of Network Security

Network security refers to the process of protecting computer networks and resources from illegal intrusion, destruction and damage through technical means and management measures. The goal of network security is to ensure the confidentiality, integrity and availability of data and to ensure the normal operation of networks and systems. According to the different protection objects and protection measures, network security can be divided into the following aspects:

Physical security: Physical security is the basis of network security, which refers to the protection of computer hardware and network equipment contact damage and authorized physical access through physical means. Physical security measures include computer room management, equipment security protection, environmental monitoring and access control. By establishing a safe physical environment, hardware equipment can be effectively prevented from being stolen, damaged and tampered.

Network security: Network security focuses on the data transmitted through the network to prevent network attacks and unauthorized security access. Network security measures include firewall configuration, network isolation, intrusion detection and prevention system (IDS/IPS), virtual private network (VPN) and network monitoring. Through network security measures, network attacks, data theft and information leakage can be effectively prevented.

System security: System security refers to protecting computer systems and their application software from vulnerability attacks and defects to ensure the normal operation of the system and the security of data. System security measures include network and application security configuration, vulnerability repair, patch management, virus protection and system monitoring. Through system security measures, the system's anti-attack capability can be improved to prevent the invasion of malware and viruses.

Data security: Data security refers to protecting the confidentiality, integrity and availability of data, and preventing data from being accessed, tampered with and destroyed without authorization. Data security measures include encryption, access control, data backup and recovery, data auditing and sensitive data protection. Through data security measures, the security of data during transmission and storage can be guaranteed, and data leakage and loss can be prevented.

Management security: Security management is to standardize the security management behavior of networks and systems through targeted formulation, security implementation strategies and management systems, and ensure the effective implementation of security measures. Security management measures include security policy formulation, security training, security auditing and emergency response. Through management security measures, the overall security awareness and security management level of the organization, and the safe operation of networks and systems can be improved.

Each aspect of network security has its specific goals and protection measures. Through the comprehensive application of these measures, a comprehensive and systematic network security protection system can be established to ensure the security and reliability of computers and network resources.

2.2 Commonly Used Network Security Technologies

In the process of ensuring network security, various technical means play an important role. The following are several commonly used network security technologies:

Firewall: Firewalls are the first line of defense for network security. They are used to control the traffic entering the network and prevent unauthorized access. Firewalls can filter and block packets that do not conform to the rules according to the default security policy, thereby preventing network attacks. Firewalls can be divided into hardware firewalls and software firewalls. Common configuration methods include packet filtering, anti-proxy and state detection. By configuring firewalls reasonably, network boundaries can be effectively protected to prevent external attacks and internal intrusions.

Intrusion Detection System (IDS): Intrusion detection systems are used to monitor network traffic in real time, detect and respond to potential security threats. IDS can be divided into network intrusion detection systems (NIDS) and host intrusion detection systems (HIDS). IDS monitors network traffic in the front. IDS identifies abnormal activities and attack behaviors by analyzing traffic characteristics and behavior patterns, and alarms and records them in time. Combined with intrusion prevention systems (IPS), defensive measures can be automatically taken after threats are detected to prevent further development of attacks.

Encryption technology: Encryption technology is used to protect the confidentiality and integrity of data and ensure the security of data transmission and storage. Commonly used encryption technologies include temporary encryption and non-temporary encryption. Temporary encryption algorithms such as AES use the same encryption key for encryption and decryption, which is fast and suitable for encryption of massive data; non-encryption algorithms such as RSA use global and private keys for encryption and decryption, which are highly secure and suitable for scenarios such as key exchange and digital signatures. Encryption technology can prevent data from being stolen, tampered with, and formatted, ensuring the secure transmission and storage of data.

Authentication technology: Authentication technology is used to confirm user identity and ensure that only legitimate users can access systems and data. Common authentication technologies include username and password, multi-authentication (MFA), and biometrics. Multi-authentication (MFA) improves the security of authentication by combining multiple authentication accounts (such as passwords, mobile SMS verification codes, biometrics, etc.) to prevent account theft and impersonation. Through authentication technology, access rights can be effectively controlled to protect the security of systems and data.

Security Information and Event Management (SIEM) System: SIEM system is used to collect, analyze, and report security incidents, providing comprehensive security cargo collection and incident response capabilities. The SIEM system integrates log and event data from multiple sources such as network devices, servers, and applications, performs real-time analysis and correlation, discovers potential security threats and abnormal behaviors, and provides alarm and emergency response solutions. Through the SIEM system, comprehensive monitoring of networks and systems can be achieved, security incidents can be discovered and handled in a timely manner, and the overall level of security management can be improved.

2.3 Network Security Standards and Regulations

Network security standards and regulations are the basis for ensuring network security, and provide organizations and enterprises with some specifications and guidelines to ensure the security and compliance of networks and systems. The following are common international and domestic network security standards and regulations:

ISO/IEC 27001: ISO/IEC 27001 is an information security management system (ISMS) standard issued by the International Organization for Standardization (ISO), which provides best practices and frameworks for information security management. The ISO/IEC 27001 standard helps organizations identify and respond to information security risks and ensure the confidentiality, integrity and availability of information through systematic risk management and control measures. By implementing the ISO/IEC 27001 standard, organizations can improve their information security management level and enhance the trust of customers and partners.

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) is a security standard jointly developed by major credit card companies to protect the security of cardholders' payment information. The PCI DSS standard requires merchants and services to focus on a series of security measures such as encryption, access control, audit logs, etc. when processing, storing and transmitting cardholder data. By complying with the PCI DSS standard, merchants can reduce the risk of payment card information leakage and protect customers' payment security.

GDPR: The General Data Protection Regulation (GDPR) is a data protection regulation enacted by the European Union to protect the personal privacy of EU citizens. GDPR sets strict requirements for the collection, processing, storage and transmission of personal data, giving data subjects more power. Companies that violate GDPR may face high fines. By complying with GDPR regulations, companies can improve data protection levels and enhance customer trust and compliance.

China's "Cybersecurity Law": The Cybersecurity Law of the People's Republic of China is China's highest comprehensive cybersecurity law, which aims to protect national cybersecurity and citizen information security. The "Cybersecurity Law" stipulates the security obligations and responsibilities of network operators, including the cybersecurity level protection system, personal information protection, and cybersecurity incident reporting. By complying with the "Cybersecurity Law", companies can improve their cybersecurity management level and ensure the security of user data and network environment.

By implementing and complying with cybersecurity standards and regulations, organizations and enterprises can establish a solid cybersecurity management system, improve security protection capabilities, and ensure the security and compliance of networks and information.

3. Application of Computer Network Security Technology in E-commerce Operation and Maintenance

3.1 Application of Firewall Technology in Operation and Maintenance

Firewall is one of the key security technologies in e-commerce systems. It controls the data flow entering and leaving the network by setting rules to prevent unauthorized access. Firewalls can filter and block data packets that do not meet the rules according to the default security policy, thereby preventing network attacks and illegal access. Firewall types include packet filtering firewalls, proxy firewalls, and state detection firewalls. Packet filtering firewalls filter data packets according to IP addresses and port numbers; proxy firewalls process data packet requests through intermediate proxy servers; state detection firewalls identify and block abnormal traffic by monitoring all active connections. After configuring a firewall, a large e-commerce platform effectively blocked multiple DDoS attacks and ensured the stable operation of the system. Through the application of firewalls, the platform can filter out a large amount of malicious traffic, reduce server load, and improve the availability and security of the system.

3.2 Application of Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) play an important role in e-commerce. IDS helps operation and maintenance personnel quickly identify and respond to potential attacks by monitoring network traffic in real time, detecting abnormal behavior and issuing alarms in a timely manner. IPS not only has detection capabilities, but also can automatically take measures when threats are found, such as blocking malicious traffic or isolating infected systems. For example, after configuring IDS/IPS, an e-commerce company successfully detected and blocked multiple SQL injections through these systems. The company can monitor and analyze network traffic in real time, discover and handle anomalies, and reduce the risk of business interruption and data leakage caused by attacks. In addition, IDS/IPS system behavior also provides detailed logs and reports to help companies investigate and analyze security incidents, further improving the level of security management.

3.3 Encryption Technology and Data Protection

The application of encryption technology in e-commerce is mainly reflected in the protection of data transmission and storage. SSL/TLS protocol is one of the most commonly used encryption technologies. By encrypting data transmission, it can effectively prevent eavesdropping and tampering of data during transmission. SSL/TLS protocol combines preset encryption and temporary encryption to ensure that data is encrypted during transmission, and only the corresponding recipient can decrypt the data. After implementing HTTPS for the entire site, an e-commerce platform has significantly improved the security of user data and increased user trust and satisfaction. In addition, the e-commerce platform also encrypts the stored data to ensure that even if the data is illegally obtained, the data content is still indispensable. Through encryption technology, the e-commerce platform can effectively protect user sensitive information and reduce the risk of data leakage.

3.4 Application of Security Protocols

The SSL/TLS protocol is one of the key technologies to protect data transmission security. In the e-commerce system, all sensitive operations such as user login and payment should be encrypted using the SSL/TLS protocol to ensure data confidentiality and responsibility. The SSL/TLS protocol prevents data from being stolen or tampered with during transmission by establishing a secure transmission channel. When users visit e-commerce websites, they can confirm the security of the connection through the "HTTPS" logo and security lock icon in the browser address bar. Through the SSL/TLS protocol, the e-commerce platform can provide a safe and reliable transaction environment to protect users' personal information and data payments. In addition, the e-commerce platform should also regularly update and manage digital certificates to ensure the validity and security of the certificates. Through the application of security protocols, the e-commerce platform not only improves the security of data transmission, but also enhances users' trust in the platform.

3.5 Case Analysis

Through actual case analysis, the application effect of network security technology in operation and maintenance is demonstrated. For example, after an e-commerce platform suffered a large-scale DDoS attack, it successfully resisted the attack and ensured the normal operation of the system by deploying a multi-layer defense mechanism. The platform first used a firewall to filter malicious traffic, and at the same time used an intrusion detection and prevention system to monitor and block abnormal behavior in real time. In addition, the platform also used content distribution network (CDN) technology to disperse network traffic and reduce the pressure on the main server. The combination of multi-layer defense mechanisms not only improved the platform's ability to defend against DDoS attacks, but also improved the overall network security level and system stability. Through these actual cases, we can see the importance and effectiveness of network technology in e-commerce security, and provide useful experience and results for other companies.

4. Evaluation of the Effectiveness of Computer Network Security Technology

4.1 Data Comparison of Security Technology Application Comparison

Evaluating the effectiveness of network security technology can be achieved through data comparison analysis. For example, a large e-commerce platform was inconsistent in the deployment of firewalls and intrusion detection systems (IDS/IPS), and there were significant differences in the changes in the number of security incidents and system downtime. Previously, the platform suffered from network attacks such as DDoS attacks and SQL injections, which caused system downtime for several hours and hundreds of security incidents reported per month. After the deployment of firewalls and IDS/IPS systems, the number of security incidents on the platform was significantly reduced, the system downtime was sharply reduced, and the average number of security incidents reported per month was the highest.

The specific data is as follows:

- Before deployment: the average number of security incidents per month was 200, and the system downtime accumulated to about 20.
- After deployment: the average number of security incidents per month was reduced to 10, and the system downtime was reduced to 2 hours.

Through these data comparisons, we can clearly see the important role of the application of network security technology in improving system security and stability. In addition, we can further analyze the changes of different types of security incidents before and after deployment to understand which threats are effectively defended and which aspects still need improvement.

4.2 User Satisfaction Survey

User satisfaction is an important indicator for evaluating the application effect of network security technology. Through the questionnaire survey, we can understand the user's satisfaction with the security and stability of the system. The questionnaire content can include the following aspects:

- System security: users' feelings about the platform's security measures, including firewalls, encryption technology, identity authentication, etc.
- System stability: users' feelings about the platform's operating stability and access speed.
- Problem handling speed: users' evaluation of the speed of security incident and fault handling.
- Overall satisfaction: users' comprehensive evaluation of the overall user experience.

For example, after a user questionnaire survey was conducted on an e-commerce platform, the data showed:

- System security satisfaction: 90% of users are satisfied with the platform's security measures.
- System stability satisfaction: 85% of users said that they did not encounter obvious system instability during use.

• Problem handling speed satisfaction: 80% of users said that when they encountered problems, the platform could respond and solve them quickly.

Through these survey results, the platform can further understand users' needs and expectations, optimize security measures and improve service quality, thereby enhancing users' trust and loyalty.

4.3 Cost-benefit Analysis

Cost-benefit analysis is an aspect of evaluating the application effect of network security technology. By comparing the investment in network security technology and the benefits brought by its cost, its economic feasibility can be evaluated. For example, the investment of an e-commerce enterprise in network security has significantly improved system security and user trust, thereby bringing business growth.

Specific analysis can include the following aspects:

• Investment costs: hardware and software procurement costs of firewalls, IDS/IPS systems, implementation and maintenance costs, training and management costs of security personnel, etc.

• Direct results: reduced number of security incidents, system downtime, reduced maintenance costs, etc.

• Indirect benefits: improved user trust, reduced user churn, increased transaction volume, improved brand image, etc.

For example, the company invested 500,000 yuan in the deployment and maintenance of network security technology in one year. Through these investments, the security and stability of the system have been significantly improved, and user trust and satisfaction have also increased. Data shows that the platform's user churn rate has dropped by 20%, transaction volume has increased by 15%, and additional business income of approximately 2 million yuan has been brought in.

Through this detailed cost-efficiency analysis, enterprises can clearly see the return on investment in network security technology, so as to better plan security strategies and allocate resources to ensure that economic benefits are maximized while ensuring security.

4.4 Conclusion

In summary, through data comparison, user satisfaction survey and cost-effectiveness analysis, the application effect of computer security technology in e-commerce operation and maintenance can be comprehensively evaluated. The effective application of security technology can not only improve the security and stability of the system, but also enhance user trust and satisfaction, thereby promoting business growth and brand image. Enterprises should continue to pay attention to the development and application of network security technology, continuously optimize security strategies, and ensure the long-term healthy development of e-commerce platforms.

5. Future Development Trends and Challenges

5.1 Application of Artificial Intelligence and Machine Learning in Network Security

With the development of artificial intelligence (AI) and machine learning (ML) technologies, the application prospects of these technologies in network security are unstable. Traditional network security technologies often rely on preset rules and signatures to detect threats, while AI and ML can improve the accuracy and efficiency of security defense by analyzing massive data, autonomously learning and identifying new threat patterns.

For example, through machine learning algorithms, network traffic and user behavior can be analyzed to discover abnormal patterns and potential threats. Deep learning technology can identify complex attack behaviors such as advanced persistent threats (APT) and zero-day attacks, thereby achieving more accurate attack threat detection and prediction. AI can also be used to automate security incident response, reduce the time of human intervention, and improve response speed and efficiency.

In the future, with the continuous advancement of artificial intelligence and machine learning technologies, network security systems will be able to adapt to and respond to complex and changing security threats more intelligently and provide a higher level of protection. However, this also brings new challenges, such as algorithm transparency, model robustness, and data privacy protection, which need to be comprehensively considered and solved in terms of technology and policy.

5.2 Security Challenges of the Internet of Things (IoT)

The rapid development of the Internet of Things (IoT) has brought new opportunities for e-commerce, but also new security challenges. IoT devices widely cover control fields such as smart homes, smart cities, and industries. The complexity of their connections and data transmission increases the difficulty of network security protection.

IoT devices usually have characteristics such as resource base, low computing power, and weak security mechanisms, which can easily become targets of attackers. Attackers can launch DDoS attacks on these devices, steal sensitive data, or invade network systems. In order to protect the security of IoT devices and data, future network security technologies need to be improved in the following aspects:

- Device authentication and identity management: Ensure that only authenticated devices can connect to the network, and prevent devices from being impersonated or tampered with through identity authentication.
- Data encryption and privacy protection: Encrypt transmitted and stored data to prevent eavesdropping and tampering of data during transmission, and protect user privacy.
- Security updates and patch management: Ensure that IoT devices can receive and install updates and patches in a timely manner to fix known security vulnerabilities.
- Threat detection and response: Detect and respond to potential security threats through real-time monitoring and analysis of IoT network traffic to prevent the occurrence and spread of attacks.

With the increasing number of IoT and the configuration of application scenarios, network security technology needs to continue to innovate and progress to cope with the ever-changing security threats and ensure the security and reliability of the IoT ecosystem.

5.3 Application of Blockchain Technology in Network Security

Blockchain technology eliminates the characteristics of decentralization, immutability and transparency, and is considered to be an effective means to enhance the security of e-commerce systems. Blockchain ensures the authenticity and integrity of data through replication and consensus mechanisms, and prevents data from being tampered with, altered and forged.

In the field of e-commerce, blockchain technology can be used in the following aspects:

- Transaction verification and traceability: Through blockchain, every transaction volume in the transaction process is recorded to achieve transaction traceability, prevent transaction interruptions and counterfeit products.
- Smart contract: Smart contract is an automated program running on blockchain, which can automatically execute contract terms when predetermined conditions are met, reduce human conflicts and disputes, and ensure the fairness and transparency of transactions.
- Data storage and sharing: Through blockchain decentralized storage technology, data can be securely stored and shared, data leakage and tampering can be prevented, and the credibility and security of data can be improved.

However, the application of blockchain technology in network security also faces some challenges, such as scalability, energy consumption and privacy protection. In the future, as technology continues to mature and optimize, the application of blockchain in network security will be more and more widely studied.

5.4 Cultivation of Network Security Talents

Network security talent cultivation is an important topic for the future development of network security. With the continuous increase of network threats and the rapid development of security technology, enterprises and organizations are increasingly in need of high-quality network security talents. How to cultivate and attract network security talents has become the key to improving network security protection capabilities.

In order to cultivate network security talents, we can start from the following aspects:

- Education and training: Strengthen the education of network security-related disciplines, set up systematic courses and training plans, and cultivate students' network security awareness and skills. Through school-enterprise cooperation, provide internships and practical opportunities to allow students to accumulate experience in actual projects.
- Professional certification: Support network security professional certification, such as CISSP, CEH, etc., to improve the professional level and professional quality of industry personnel and enhance their competitiveness in the job market.
- Continuous learning and development: Network security technology is developing rapidly, requiring industry personnel to continuously learn and update their knowledge. By participating in training, seminars and industry conferences, understand the latest security technologies and development trends, and maintain technological leadership.
- Motivate and retain talents: By providing compensatory salaries and benefits, a good working environment and career development opportunities, we can attract and retain outstanding cybersecurity

talents and improve the overall level of the team.

Through multi-level and multi-channel talent training strategies, we can provide enterprises and society with a large number of high-quality cybersecurity talents and improve the overall cybersecurity protection capabilities.

6. Conclusion

This paper analyzes the application of computer network security technology in e-commerce operation and maintenance, and demonstrates the role of these technologies in improving system security and stability. Despite the sudden challenges, with the continuous development and progress of technology, network security technology can better cope with complex and changing security threats and ensure the health and sustainable development of business through continuous innovation and optimization of e-commerce security technology and the cultivation of high-quality network security talents.

References

Cai, X. Y. (2023). Application of computer network security technology in e-commerce. *Electronic Technology*, *52*(08), 212-213.

Cheng, X. Y. (2024). Effective application of computer network security technology in e-commerce operation and maintenance. *Science and Technology Innovation and Application*, *14*(13), 171-174. http://doi.org/10.19981/j.CN23-1581/G3.2024.13.041

Cui, X. M, & Tian, S. Y. (2024). Application of computer network security technology in e-commerce. *Information and Computer (Theoretical Edition)*, *36*(05), 221-223.

Dai, X. M. (2023). Application of computer network security technology in e-commerce. *China Management Informationization*, *26*(12), 191-193.

Guo, J. Z. (2022). Application of computer network security technology in e-commerce. *Network Security Technology and Application*, *2022*(03), 98-99.

He, C. H. (2020). Discussion on the application of computer network security technology in e-commerce. *Digital World*, 2020(12), 255-256.

He, W., Wang, H., He, J. Y., et al. (2021). Discussion on the application of computer network security technology in e-commerce. *Information Recording Materials*, *22*(12), 123-124. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2021.12.031

Lin, Z. Z. (2021). Research on the application of computer network security technology in e-commerce. *Network Security Technology and Application, 2021*(05), 139-141.

Liu, B. (2021). On the application of computer network security technology in e-commerce. *Information Recording Materials*, *22*(10), 138-139. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2021.10.066

Liu, W. (2021). Electronic Analysis of the application of computer network security technology in business. *Network Security Technology and Application*, *2021*(12), 129-130.

Song, Y. F. (2021). Computing Application of computer network security technology in e-commerce. *Marketing World*, *2021*(24), 38-39.

Wang, Y. J., & Wang, P. (2023). Application of computer network security technology in e-commerce environment. *China New Communications*, *25*(21), 120-122.

Wu, B. R. (2023). Application of computer network security technology in e-commerce. *Electronic Technology*, *52*(10), 268-269.

Wu, R. (2022). Analysis of the application of computer network security technology based on e-commerce environment. *Computer Knowledge and Technology*, *18*(10), 31-33. http://doi.org/10.14004/j.cnki.ckt.2022.0757

Xiong, N. (2021). Analysis of the application of computer network security technology in e-commerce. *Network Security Technology and Application*, *2021*(04), 99-100.

Yang, J. R. (2021). Application of computer network security technology in e-commerce. *Electronic Technology and Software Engineering*, *2021*(17), 259-260.

Zhang, F. (2023). Application of computer network security technology in e-commerce. *Network Security Technology and Application*, *2023*(05), 135-137.

Zhang, Q. S. (2021). Application of computer network security technology in e-commerce. *Electronic Technology and Software Engineering*, *2021*(11), 236-237.

Zhang, Y. M. (2020). Application of computer network security technology in e-commerce. *Information and Computer (Theoretical Edition)*, *32*(15), 198-200.

Zou, C. (2023). Application of computer network security standardization technology in e-commerce. *Popular Standardization*, *2023*(18), 148-150.