Journal of Computing and Electronic Information Management
ISSN: 2413-1660 | Vol. 16, No. 2, 2025

Research on Computer Information Network Security Technology and Development Direction

Yue Xu

Salesforce Service Cloud, Redmond,98052, USA
yxu.joyce@gmail.com

Abstract: With the rapid development of information technology, the research and application of computer information network security technology has become the key to guarantee the healthy development of the information society. Currently, the field of network security is in a stage of rapid technological innovation, and it is particularly important to conduct in-depth research on traditional security means such as encryption technology, intrusion detection, access control, etc., and to build a more advanced and intelligent security protection system by combining emerging technologies such as artificial intelligence and blockchain. Encryption technology continues to make progress in terms of complexity and efficiency, firewalls are gradually developing in a more intelligent direction, and intrusion detection systems are significantly improving in terms of adaptive capabilities. In addition, the introduction of artificial intelligence makes security protection more dynamic and precise, and blockchain provides a new guarantee mechanism for data integrity and transparency. The rapid expansion of the Internet of Things (IoT) and the wide application of cloud computing have brought new directions and challenges to network security technologies. In terms of privacy protection, new technological means are emerging to provide a stronger guarantee for personal data security. This study aims to provide comprehensive theoretical guidance and practical reference by analyzing the above technologies in depth and looking forward to the future development trend of network security.

Keywords: Computer information network security; Cryptography; Intrusion detection; Directions for development.

1. Introduction

As the digital revolution accelerates, the security of computer information networks has increasingly become a focal point of global attention. The information network has profoundly influenced various domains, including finance, healthcare, manufacturing, et cetera, and the gravity of security issues cannot be overstated. A plethora of security threats exist, ranging from traditional viruses and hacker attacks to sophisticated cyber-espionage activities, encompassing a wide spectrum of network dimensions. Consequently, the study of computer information network security technologies and their developmental trajectories holds significant practical importance and long-term strategic value. Within information security strategies, critical technologies such as encryption, firewalls, intrusion detection systems, and access control have long served as the bedrock of defense. With the ever-evolving network environment, the capacity to address emerging threats demands continuous enhancement. In recent years, the emergence of artificial intelligence and blockchain, coupled with the accelerated proliferation of the Internet of Things, has introduced revolutionary changes to cybersecurity. These emerging technologies not only transform traditional security strategies but also prompt extensive contemplation on new directions in security technology. This article will, on the basis of examining the current technological landscape, explore the dynamic trends of future development.

2. Overview of Computer Information Network Security

The rapid development of the information network has not only brought convenience and efficiency but has also rendered the task of safeguarding information security more arduous and intricate. The objective of cybersecurity is to protect the confidentiality, integrity, and availability of information, defending against various types of security threats and attacks, such as hacking, malware, and data breaches. In response to these challenges, security measures at various levels have emerged, including encryption technologies, firewalls, intrusion detection systems, and access control, forming a robust network defense system. At the heart of encryption technology is the protection of data from theft and tampering during transmission, involving complex algorithms and key management. Traditional firewalls, as the first line of defense, have continuously expanded and evolved to counter increasingly sophisticated attack scenarios. Intrusion detection systems can not only identify known attacks but also learn new threat patterns, becoming an integral part of the dynamic defense in cybersecurity. Furthermore, access control technologies ensure that only authorized users can access specific network resources through authentication and permission management. Cybersecurity is not merely a technical challenge but also a cultural and awareness challenge. Every participant in the network must strengthen their security awareness and assume corresponding responsibilities to cope with the ever-changing cyber threats. This concerns not only individual information security but also directly impacts the security and stability of the entire information society.

3. Research on computer information network security technology

3.1. Encryption Technology

Encryption technology stands as the cornerstone of cybersecurity within computer information networks, bearing the vital responsibility of safeguarding information from unauthorized access during transmission and storage. In

recent years, significant breakthroughs have been made in the realms of complexity and efficiency in encryption. Symmetric and asymmetric encryption constitute the primary methodological frameworks; symmetric encryption, with its rapidity and efficiency, is well-suited for the real-time protection of substantial data volumes, whereas asymmetric encryption, characterized by its distinct public and private key structure, is widely employed in secure communications and digital signatures, ensuring the confidentiality and integrity of data. The looming threat of quantum computing undoubtedly heralds a formidable challenge for the field of encryption, simultaneously serving as a catalyst for the innovation of encryption technologies. Traditional encryption algorithms are rendered vulnerable in the face of the formidable computational power of quantum computing, prompting researchers to delve into quantum-safe algorithms and quantum key distribution techniques to secure the future of information safety. These technologies leverage the principles of quantum physics, utilizing uncloneable qubits for key distribution, thereby offering unprecedented security assurances. With the proliferation of the Internet of Things and cloud computing, the demand for novel encryption technologies has become increasingly pressing, propelling the gradual development of lightweight encryption techniques within edge computing environments. Such techniques must provide ample security within resource-constrained settings, ensuring that, regardless of the complexity of the network environment, the protection of users' data and privacy remains reliably steadfast. Encryption technology transcends mere technical competition; it embodies the foundational belief in safeguarding the security of the digital society [1].

3.2. Firewall Technology

Firewall technology plays an indispensable role in the security of computer information networks, serving as the guardians of cybersecurity. These "gatekeepers" are tasked with monitoring and controlling the flow of data traffic into and out of networks. Traditional firewalls primarily rely on packet header information for filtering and forwarding, a method that is highly effective against simple attacks. However, as network threats have become more sophisticated, attackers have become increasingly adept at disguising malicious traffic to evade firewall detection. Consequently, modern firewall technology has incorporated features such as deep packet inspection and application layer filtering. The advent of Next-Generation Firewalls (NGFW) marks a significant leap forward in firewall technology. These advanced firewalls not only integrate traditional packet filtering capabilities but also introduce sophisticated functionalities such as intrusion detection and prevention systems, application recognition, user identity management, and more. This enables more precise and flexible cybersecurity strategies. The application of machine learning and artificial intelligence technologies further enhances the firewall's intelligence, allowing it to autonomously analyze and identify anomalous traffic, thereby enabling a more proactive defense. With the widespread adoption of cloud computing and the Internet of Things, firewalls are evolving towards "cloud firewalls" and "virtual firewalls," offering protection capabilities across platforms and networks. This transformation not only meets the demands of new network architectures but also strengthens defenses against distributed attacks.

3.3. Intrusion detection and defense system

Intrusion Detection and Prevention Systems (IDPS) play an indispensable role in safeguarding the security of computer information networks. These systems serve as the "alarm system" of the network, possessing the capacity to not only detect anomalous activities in real-time but also to autonomously respond to potential threats. In the face of increasingly sophisticated network attacks, IDPS technology has evolved continuously, transitioning from initial detection based on known threat signatures to advanced detection methodologies that employ behavioral analysis and pattern recognition. Modern IDPS systems leverage machine learning and big data analytics to facilitate the real-time processing of vast amounts of network data, thereby significantly enhancing their ability to detect unknown threats. By establishing a baseline through the analysis of normal network behavior, IDPS can more accurately identify anomalous actions, swiftly detecting zero-day attacks and advanced persistent threats (APTs). This predictive defensive capability surpasses that of traditional cybersecurity measures. Beyond the enhancement of detection capabilities, intrusion prevention systems have fortified their automated response mechanisms. Upon identifying a threat, these systems can promptly block malicious traffic, adjust firewall rules, and even notify administrators to prevent the escalation of threats. To accommodate the widespread adoption of cloud computing and virtualization, IDPS technology is also evolving towards virtualization, offering more flexible deployment options and scalability. Through continuous technological innovation, IDPS not only amplifies the depth of network security but also bolsters the overall awareness of the security landscape within the network environment [2].

3.4. Access Control Technology

Access control technology is a core component of computer information network security, providing a solid safeguard to protect data and systems from unauthorized access. This technology is based on ensuring that only authenticated and authorized users are granted the necessary access to resources. Traditional access control methods usually include role-based access control (RBAC) and mandatory access control (MAC)-based access control. Although these methods solve the problem of privilege assignment to a certain extent, they appear to be somewhat incompetent in the face of modern complex and dynamic network environments. As the degree of informatization increases, fine-grained and dynamic access control mechanisms are especially important. Attribute-based access control (ABAC) has gradually become an attention-grabbing technology, which utilizes multiple dimensions such as user attributes, resource characteristics and environmental conditions to make permission judgments. This flexibility greatly enhances the adaptability of the system, especially in enterprise cloud environments and distributed networks, and can provide more precise permission management for diverse access needs. The rise of zero-trust architecture also brings a new perspective to access control technology, which emphasizes that it no longer relies on traditional network trust boundaries and that any access request must be strictly authenticated and authorized. This concept subverts the original security model and provides new ideas and technical realization paths for dealing with internal and external threats. In addition, the combination of identity management and access control is widely used in modern security practices,

providing features such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) to enhance access security and user experience.

4. Development direction of computer information network security technology

4.1. Application of Artificial Intelligence and Machine Learning in Network Security

The application of artificial intelligence and machine learning in cybersecurity has emerged as a formidable force of innovation within the realm of information security. These technologies offer novel methodologies to address increasingly intricate cyber threats, significantly enhancing the efficiency and accuracy of network defense. Artificial intelligence-based cybersecurity solutions possess the capacity to automate threat detection, analyzing vast quantities of data to uncover concealed patterns of attack, thereby substantially mitigating security risks stemming from human error. In the realm of anomalous network traffic detection, machine learning algorithms are trained on extensive historical datasets to establish a baseline model of normal network behavior. Consequently, when abnormal traffic occurs, the system can swiftly identify and raise alerts, affording the security team invaluable response time. This capability for real-time analysis is particularly crucial in the face of rapid and diverse cyber assaults. Furthermore, AI-driven security measures extend to intrusion detection, malware analysis, and vulnerability scanning. These intelligent systems not only identify known threats but also unearth unknown risks, even predicting their likelihood prior to their execution. By adopting adversarial machine learning techniques, security teams can better comprehend the methodologies of attackers, thereby formulating more effective defensive strategies. It is imperative to note that relying solely on artificial intelligence and machine learning is insufficient; the advancement of technology must be harmonized with the insight of human analysts to enhance discernment and facilitate complex strategic decision-making. This paradigm of human-machine collaboration is poised to be a prevailing trend in the evolution of cybersecurity, not only augmenting system defenses but also infusing the information security sector with renewed vitality and hope [3].

4.2. Application of blockchain technology in network security

Blockchain technology is gradually changing the landscape of cybersecurity with its decentralized and tamper-proof characteristics. With the support of distributed ledger structure, the storage and transmission of data become more transparent and secure, and every transaction and change of information is accurately recorded and difficult to forge, which is of great significance in preventing data tampering and information leakage. In identity verification, blockchain can provide a more secure and efficient solution. While traditional identity management systems are susceptible to single points of failure and attacks, the decentralized nature of blockchain allows the storage and verification of identity information to be independent of a single institution, thus reducing the risk of attack. Users can realize autonomous identity management with the help of blockchain, which enhances privacy protection. In the face of cyber-attacks, the smart contract feature of blockchain offers the possibility of automated response. These contracts can automatically detect and handle anomalous behavior based on predefined rules, helping to stop potential attacks in time. At the same time, multiple nodes jointly participate in the process of recording and verifying network activities, making it more difficult for attackers to carry out attacks. The consensus mechanism ensures the uniqueness and authenticity of the data, thus effectively preventing the double spend problem. Blockchain technology also excels in data integrity auditing, allowing enterprises to conduct independent audits by accessing the blockchain's history without having to trust a third-party auditor. However, blockchain is not omnipotent, and performance bottlenecks and challenges of scaled application still exist, but with the continuous evolution of the technology, the prospect of its application in the field of cybersecurity is undoubtedly very broad, and provides a solid foundation for the establishment of trust [4].

4.3. Internet of Things (IoT) Security

The security of the Internet of Things (IoT) constitutes a significant challenge within the realm of cybersecurity. With billions of devices interconnected, safeguarding these devices from malicious assaults has become imperative. The profusion and dispersion of these devices, often characterized by limited resources and delayed updates, inadvertently create opportunities for attackers. Numerous IoT devices lack robust security mechanisms, thereby rendering them susceptible to potential network breaches, and even triggering large-scale Distributed Denial of Service (DDoS) attacks. In ensuring IoT security, the foremost tasks are to guarantee device authentication and the encryption of data transmission. Whether pertaining to smart home devices or industrial sensors, securing communication links is pivotal in thwarting man-in-the-middle attacks. Unencrypted data can be easily intercepted and tampered with. Concurrently, the firmware update mechanism for devices must be fortified to promptly address security vulnerabilities. Implementing automated and secure update processes effectively mitigates the risks associated with human error. Network segmentation also emerges as a crucial strategy in protecting IoT devices. By isolating IoT devices into separate networks, even if individual devices are compromised, it prevents attackers from easily accessing other critical systems. Moreover, real-time monitoring and anomaly detection technologies are indispensable, aiding in the swift identification and response to unusual activities, thereby minimizing potential harm from attacks. Despite the formidable challenges, the future of IoT security holds promise. The application of artificial intelligence in the security domain is actively propelling the evolution of IoT security. Integrating security into every phase of device design and development not only enhances overall network security but also bolsters user trust in IoT applications.

4.4. Cloud computing security

The multi-tenant architecture of cloud computing environments renders data isolation and privacy protection particularly paramount, as users must be assured that their data will not be compromised due to shared infrastructure. Data encryption plays a pivotal role in cloud security strategies; whether concerning static data or data in transit, encryption measures ensure that even if data is intercepted, it remains inscrutable to attackers. The significance of access

control mechanisms is self-evident, permitting only authorized users to access resources; this necessitates robust authentication and rights management systems to avert unauthorized access. Security concerns extend beyond mere data protection; the dynamic nature of cloud computing also faces potential threats such as virtual machine escape, API vulnerabilities, and distributed denial-of-service attacks. In addressing these challenges, the importance of security monitoring and threat detection technologies is magnified, as deploying real-time monitoring tools enables the timely identification of anomalous activities and swift responses. To enhance the reliability of cloud services, the adoption of a multi-layered security architecture along with regular security audits is indispensable. The delineation of responsibilities between cloud service providers and users must also be clearly articulated, fostering close collaboration to ensure the implementation and compliance of security policies. Looking ahead, with the evolution of cloud computing technology, the application of a zero-trust architecture will further bolster security protections by continuously enhancing access control and traffic analysis, thereby cultivating a more secure cloud environment [5].

4.5. Privacy Protection Technology

Privacy protection technologies have emerged as a focal point in today's digital era. With the relentless escalation of data collection and utilization, the conundrum of safeguarding individual privacy while enjoying the conveniences of technology has become a subject of significant attention. At the heart of privacy protection lies the meticulous balancing act of minimizing the exposure of personal information while sustaining the practical value of data. Differential privacy stands out in this context, offering a unique advantage by injecting random noise into data, thereby ensuring that external observers are unable to trace back to specific personal information. Homomorphic encryption, a promising technique, permits computations directly on encrypted data, substantially elevating the level of privacy protection. This methodology ensures that even during data processing, service providers are unable to access raw data, effectively eliminating the risk of data breaches. When delving into blockchain technology, zero-knowledge proofs ensure both privacy and the authenticity of transactions. Users can substantiate the truth of a claim without disclosing any supplementary information, thereby enhancing the integrity of the system. User-controlled data management platforms are increasingly gaining prominence. These platforms empower users with ownership and sharing rights over their data, enabling them to oversee which data is accessed and how it is utilized through granular permission management, thus enhancing transparency and trustworthiness. Moving forward, the further evolution of privacy protection technologies necessitates interdisciplinary collaboration. This advancement hinges not only on technical breakthroughs but also on the concerted efforts of law, ethics, and industry standards.

5. Conclusion

In this era of ever-increasing complexity in information technology, ensuring cybersecurity has become a sophisticated and urgent endeavor. The interweaving of current technologies and the emergence of novel innovations continually expand the breadth and depth of cybersecurity. The application of artificial intelligence renders security measures more intelligent and precise, while the decentralized nature of blockchain technology offers innovative solutions for data integrity. The challenges of IoT security have spurred more meticulous research into device and network interactions, and the solutions to cloud computing security issues are gradually maturing. Moreover, the advancement of privacy-enhancing technologies safeguards the security of user data and protects personal privacy from infringement. Moving forward, the development of cybersecurity technologies will need to balance innovation and practicality, continuously adapting to new technological landscapes and evolving demands. Remaining vigilant to emerging threat patterns and technological innovations will render cybersecurity strategies more comprehensive and effective, laying a solid foundation for the stability and sustainable development of the information society.

References

[1] Cheng K.Internet of Things (IoT) Computer Network Security and Its Remote Control Technology: Key Points and Applications[J].Frontiers in Computing and Intelligent Systems, 2024, 9(1):14-16.

[2] Ge D,Fang Q ,Han Q .Utilization and Security Protection of Computer Communication Technology in the Information Age[J].Journal of Electronics and Information Science, 2024, 9(2):22.

[3] XingK.A Practical Study of Big Data Technology in Computer Network Information Security Processing [J].Journal of Electronic Research and Application, 2023,7(6):36-41.

[4] Lin Y.Analysis of the Application of Computer Information Technology in Network Security under the Background of Big Data[J].Advances in Computer and Communication, 2023, 4(1):19.

[5] Yina Q.Probe into Computer Network Information Security and Protection Strategy in the Age of Big Data[J].The Frontiers of Society, Science and Technology, 2022, 4(11):12.