International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 8, Number 6, Year 2026
DOI: https://doi.org/10.62051/ijcsit.v8n6.04
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Network and Information Security

Guanghao Zhang

School of Intelligent Manufacturing, Guangzhou Huali College, Jiangmen, China

ABSTRACT

This paper provides a systematic review and comprehensive analysis of network and information security, addressing the complex threats currently confronting cyberspace. Starting from an examination of various types of cyber attacks and their technical characteristics, and incorporating case studies of typical security incidents, this paper reveals the evolution trends in attack methodologies and their impact on critical information infrastructure. At the technical level, this study constructs an information security technology framework centered around encryption and authentication technologies, as well as intrusion detection and defense mechanisms, while exploring implementation pathways for multi-layered security protection. At the management and policy level, this study introduces a security risk assessment methodology, discusses the processes of risk identification, quantification, and hierarchical control, and proposes optimization recommendations regarding the establishment of security policies and emergency response mechanisms. This paper aims to serve as a reference for technical architecture design and security governance practices within the field of network and information security, while providing theoretical support for enhancing overall security protection capabilities and risk mitigation capabilities.

KEYWORDS

Cybersecurity; Information Security Technology Framework; Cyber Attacks; Intrusion Detection and Prevention; Security Risk Assessment

1. INTRODUCTION

Network and information security is a critical domain for protecting computer networks and data from unauthorized access and attacks. In recent years, driven by the rapid advancement of information technology, cybersecurity threats have become increasingly severe, encompassing malware, phishing attacks, denial-of-service (DDoS) attacks, and Advanced Persistent Threats (APTs). According to the 2022 Cybersecurity Report, global economic losses resulting from cyberattacks have reached $600 billion, with 95% of cybersecurity incidents originating from human error.

A cybersecurity framework typically comprises three core elements: confidentiality, integrity, and availability (the CIA triad). Confidentiality ensures that only authorized users can access relevant data, usually implemented using encryption algorithms such as AES or RSA; integrity is maintained through hash functions like SHA-256 to verify data integrity during storage and transmission, ensuring that the data has not been tampered with; availability focuses on ensuring that the system can operate normally when needed, often involving the application of redundancy design and load balancing techniques.

Cybersecurity protection measures can be categorized into three major types: physical security, network security, and application security. Physical security involves physical protection measures for data centers and equipment, such as implementing video surveillance and access control systems; network security utilizes tools like firewalls, Intrusion Detection Systems (IDS), and Intrusion

Prevention Systems (IPS) to establish network boundaries, while employing traffic analysis and anomaly detection to prevent network attacks; application security emphasizes the integration of security measures throughout the software development lifecycle, commonly including SQL injection protection and Cross-Site Scripting (XSS) attack prevention techniques.

When implementing network and information security policies, enterprises should adhere to a risk management framework by identifying potential risks, assessing their impact, and establishing corresponding governance mechanisms. By employing risk assessment models such as NIST SP 800-30 and ISO 27005 to conduct vulnerability assessments on critical assets, and integrating these findings with common CVE (Common Vulnerabilities and Exposures) databases, enterprises can promptly apply patches to reduce the attack surface. Additionally, enterprises should conduct regular security audits and penetration tests to ensure the effectiveness of their security policies.

Regarding compliance, enterprises must adhere to international regulations such as the GDPR and HIPAA to protect user privacy and data security. It is essential to enhance employee training on security awareness to reduce internal security vulnerabilities resulting from social engineering attacks; furthermore, information-sharing mechanisms should not be overlooked, as threat intelligence sharing across industries can help elevate overall protection levels.

Future development trends point toward the application of artificial intelligence (AI) and machine learning (ML) in cybersecurity; these technologies are capable of automatically detecting and responding to anomalous behavior, thereby reducing the need for manual intervention. For example, using AI algorithms to analyze network traffic patterns can help identify potential attack behaviors. The rise of quantum computing will also pose challenges to traditional encryption algorithms, driving research into more secure encryption schemes.

Against the backdrop of the explosive growth of the Internet of Things (IoT), cybersecurity will face new challenges posed by smart devices, with device identity authentication, data protection, and network isolation becoming critical issues. The integration of dynamic security policies, container technology, and microservices architecture will provide solutions for flexibly addressing complex network environments.

Overall, network and information security is an ever-evolving field that requires specialized professionals and continuous technological innovation to address dynamic threats and challenges.

2. CYBERSECURITY THREAT ANALYSIS

2.1. Types and Characteristics of Cyber Attacks

Cyberattacks can be classified based on their attack methods, objectives, and impact, primarily including types such as malware, Denial-of-Service (DoS) attacks, Man-in-the-Middle (MitM) attacks, phishing, and data breaches.

Malware refers to programs designed to achieve their objectives by compromising or interfering with computer systems, networks, and user data. Common types of malware include viruses, worms, trojans, and ransomware. Viruses spread by self-replicating and infecting other programs; a typical example is the ILOVEYOU virus. Worms can propagate independently without requiring a host file; an example is the Morris worm. Trojans disguise themselves as legitimate programs—such as the Emotet Trojan—and are often used to steal user credentials. Ransomware encrypts files to demand a ransom; a prime example is WannaCry, which caused losses exceeding $4 billion.

A Denial-of-Service (DoS) attack aims to render a target network or service unable to function normally, thereby preventing legitimate users from accessing it. Its variant, the Distributed Denial-of-Service (DDoS) attack, employs a large number of compromised devices to launch an attack, with the attack traffic potentially reaching several Tbps; common attack methods include SYN floods,

UDP floods, and HTTP request floods. These attacks not only impair service availability but may also lead to economic losses and reputational damage. For example, in 2016, a massive DDoS attack targeting the DNS service provider Dyn caused multiple websites, including Twitter and Netflix, to go offline.

In a Man-in-the-Middle (MitM) attack, the attacker eavesdrops on or tamper with the communication between two parties, typically by exploiting insecure public Wi-Fi networks or forging certificates. The attacker can employ techniques such as SSL stripping or ARP spoofing to insert malicious scripts or steal sensitive information. The success rate of a MitM attack is closely tied to the users security awareness and the complexity of the network environment.

Phishing attacks involve stealing usernames and passwords by forging emails or websites. These attacks often employ social engineering techniques to trick users into clicking malicious links and entering sensitive information. According to a 2019 report, approximately 90% of data breach incidents were caused by phishing attacks. Among the various variants of phishing attacks, CEO fraud and email subdomain spoofing have emerged as increasingly prevalent attack methods in recent years; therefore, it is essential for enterprises to conduct security training to enhance employee vigilance.

Data breaches involve unauthorized access to sensitive data, typically occurring due to technical vulnerabilities, employee errors, or malicious actions by insiders. In the 2017 Uber data breach incident, information of approximately 57 million users and drivers was compromised; insufficient security measures and delayed patching of the vulnerabilities resulted in extremely severe consequences. The direct economic losses arising from data breaches include not only compensation payments to customers but also legal liabilities and damage to brand reputation.

In recent years, the widespread adoption of 5G networks and the proliferation of IoT devices have expanded the scope of cyberattacks, giving rise to a constant stream of new attack techniques. Attackers are leveraging AI and machine learning technologies to enhance their attack effectiveness and execute sophisticated locking attacks. Furthermore, the emergence of quantum computing may pose a threat to existing cryptographic algorithms; therefore, it is essential to maintain continuous vigilance regarding developments in the field of cybersecurity and strategies for addressing emerging threats.

Governments and enterprises should strengthen infrastructure security in their cybersecurity defenses by conducting regular security audits and penetration testing, implementing a multi-layered defense strategy, ensuring timely updates and patches for system vulnerabilities, providing regular security training for employees, and enhancing their security awareness. Additionally, the comprehensive implementation of data encryption and access control mechanisms serves as a crucial measure for reducing the risk of data breaches.

2.2. Typical Security Incident Cases

In recent years, network and information security incidents have occurred frequently; the following section presents several typical cases, analyzes their attack methodologies and corresponding protection measures, and identifies potential security vulnerabilities and risks.

In 2017, the "WannaCry" malware exploited a vulnerability in the Windows operating system (CVE-2017-0144), which stemmed from an implementation flaw in the SMB protocol; this security incident affected approximately 200,000 computers across more than 150 countries. Attackers used ransomware to encrypt users files and demanded a ransom of approximately $300 in Bitcoin. The incident caused hospitals, businesses, and government agencies worldwide to experience operational paralysis, and the widespread response to this event prompted Microsoft to release an emergency patch update for older versions of its operating systems.

In 2018, the "Facebook data breach" incident exposed severe flaws in the companys ability to properly protect user data, affecting more than 87 million users. Due to improper API permission management and the abuse of third-party applications, users private information was collected and maliciously exploited. To address these damages, Facebook implemented a series of remedial measures—including revising its privacy policy and strengthening its data sharing review process—to enhance transparency and rebuild user trust.

In 2020, the "SolarWinds hack" posed a severe threat to global infrastructure, as attackers successfully gained access to SolarWinds Orion IT management platform and implanted malicious code. This incident affected several critical government agencies, including the U.S. Department of the Treasury and the Department of Defense; through supply chain attacks, the attackers exploited the code signing mechanism to bypass security protections and implant backdoors for remote control. To mitigate the impact of the attack, enterprises implemented a series of protective measures, such as updating the Orion software, enhancing login monitoring, and strengthening access controls.

The "Colonial Pipeline ransomware attack" that occurred in 2021 involved attackers who exploited weak passwords on a VPN to perform brute-force attacks, thereby gaining administrative access to the companys network and severely disrupting fuel supplies along the U.S. East Coast. The attackers demanded a ransom exceeding $4.4 million; ultimately, the company paid part of the ransom to swiftly restore its operations. This incident sparked widespread discussions regarding cybersecurity for critical infrastructure and prompted governments to enact new legislation and adjust their policies concerning supply chain security.

In 2022, the "Log4j vulnerability" became a focal point of global cybersecurity attention. This vulnerability (CVE-2021-44228) affected the Apache Log4j library; attackers exploited this vulnerability to achieve remote code execution, impacting thousands of services. Major enterprises were forced to urgently update their servers and applications to patch the security vulnerability. This incident highlighted the widespread adoption of open-source software in enterprises and its associated potential risks.

In 2023, during the "China Telecom Locust Attack" incident, the hacker group Asnar Estonia Team launched a DDoS attack against certain servers of China Telecom, with the peak traffic volume of a single attack reaching 500 Gbps. The incident disrupted network services for several hours, affecting hundreds of thousands of users. China Telecom implemented technical measures such as traffic scrubbing and enhanced source address verification to restore normal operations. Meanwhile, this incident also prompted a review and improvement of the network protection mechanisms employed by ISPs.

Each security incident exposes weaknesses in system design and management, while simultaneously driving advancements in cybersecurity technologies and the refinement of relevant policies. Continuously strengthening security safeguards and promptly updating security protection strategies has become an effective approach for addressing potential security incidents.

3. INFORMATION SECURITY TECHNOLOGY FRAMEWORK

3.1. Encryption and Authentication Technologies

Encryption and authentication technologies form the core components of information security protection, involving a variety of algorithms and protocols designed to ensure data confidentiality, integrity, and identity verification. Symmetric encryption and asymmetric encryption are the two fundamental encryption methods. Symmetric encryption uses the same key for both encryption and decryption; commonly used algorithms include AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard). AES supports key lengths of

128 bits, 192 bits, and 256 bits, providing a balance between encryption strength and efficiency, and is widely adopted for data protection.

Asymmetric encryption uses a pair of keys: the public key is used for encryption, while the private key is used for decryption. RSA (Rivest–Shamir–Adleman) is the most widely used asymmetric encryption algorithm; its security relies on the integer factorization problem, with key lengths typically being 2048 bits or higher. ECC (Elliptic Curve Cryptography) provides comparable security with much shorter keys—key lengths as short as 256 bits—making it particularly well-suited for mobile devices.

In data transmission, the SSL/TLS protocol is widely used to enable secure communication. The TLS (Transport Layer Security) protocol provides the authentication and encryption required to establish a secure connection by utilizing symmetric encryption, asymmetric encryption, and hash functions. The handshake process in SSL/TLS involves verifying identities through digital certificates, performing key exchange using RSA, and ultimately encrypting session data using symmetric encryption.

Identity authentication technologies ensure the authenticity of both communicating parties; common methods include knowledge-based authentication (such as passwords), token-based authentication (such as one-time passwords, OTP), and biometric authentication (such as fingerprint or facial recognition). OAuth and OpenID Connect provide respective token-based authentication solutions that enable third-party applications to securely access user resources without exposing user credentials.

In key management, the generation, storage, distribution, and destruction of encryption keys are critical. Common key management standards such as PKCS #11 and ISO/IEC 27001 ensure the security of the entire key lifecycle. Hash algorithms (such as SHA-256) are employed to ensure data integrity; by comparing the hash values, it can be determined whether the data has been tampered with.

Hybrid encryption technology combines the advantages of both symmetric and asymmetric encryption and is commonly used for secure message transmission and data storage. A common implementation involves using asymmetric encryption to generate a session key, which is then used for symmetric encryption. This approach not only ensures the security of key transmission but also enhances the efficiency of data encryption.

Key exchange protocols such as Diffie-Hellman can securely share cryptographic keys over insecure channels, thereby mitigating eavesdropping risks. Quantum Key Distribution (QKD) technology leverages principles of quantum mechanics to achieve the absolute secure distribution of cryptographic keys, offering promising prospects for future applications.

Future cryptographic technologies should focus on addressing the challenges posed by quantum computing; research into post-quantum encryption algorithms is currently underway to ensure data security in quantum computing environments. Furthermore, the integration of dynamic authentication and adaptive encryption techniques with artificial intelligence offers new directions and solutions for securing modern information systems.

3.2. Intrusion Detection and Prevention

Intrusion detection and prevention are vital components of information security, with their primary objective being to promptly detect and respond to unauthorized access and attacks against computer networks and systems. Intrusion Detection Systems (IDS) can be categorized into two main types: signature-based detection and anomaly-based detection. The former identifies intrusions by comparing network traffic against a known signatures database, whereas the latter identifies anomalies using a normal traffic model. IDS deployment modes include Network-Based IDS (NIDS)

and Host-Based IDS (HIDS); the former monitors all network traffic, while the latter focuses on individual hosts.

Currently popular IDS solutions include Snort, Suricata, and OSSEC. Snort, an open-source network intrusion detection system, utilizes a flexible rule syntax for writing detection rules, supports real-time traffic analysis and logging, and incorporates protocol analysis and content matching capabilities. Suricata enhances its multi-threaded processing capabilities, supports higher traffic throughput, and provides Deep Packet Inspection (DPI) technology. OSSEC, on the other hand, is a host-based intrusion detection tool that leverages technologies such as File Integrity Monitoring (FIM) and Registry Monitoring to provide comprehensive security monitoring.

The Intrusion Prevention System (IPS), as an extension of the Intrusion Detection System (IDS), possesses active defense capabilities; upon detecting malicious activity, it can automatically take measures to block the attack. IPS typically employs methods such as traffic interception and connection reset to effectively mitigate the impact of attacks. Furthermore, by integrating with technologies such as firewalls and Web Application Firewalls (WAFs), IPS forms a multi-layered defense strategy that enhances overall network security protection capabilities.

Modern intrusion detection and prevention systems do not rely solely on a single technology but require the integrated application of multiple approaches. Machine learning-based detection methods have gradually become a research focus, leveraging algorithms such as Support Vector Machines (SVM) and decision trees to enhance both detection accuracy and response speed. Deep learning methods, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory networks (LSTM), have demonstrated excellent performance in pattern recognition and time-series analysis; among these, LSTM is particularly well-suited for processing time-series data.

Key technical metrics include the False Positive Rate (FPR) and the False Negative Rate (FNR). When optimizing the model, it is essential to balance these two parameters to enhance the systems practicality. During the deployment process, a hierarchical approach should be adopted: first, perform asset identification; next, conduct risk assessment and strategy formulation; and finally, implement monitoring and response mechanisms.

The challenges associated with intrusion detection and defense cannot be overlooked; network attack methods are becoming increasingly sophisticated, with attackers employing encryption techniques, spoofed traffic, and novel vulnerabilities to bypass detection mechanisms. Therefore, it is crucial to continuously update detection rules and databases, necessitating the implementation of a dynamic update mechanism. The integration of automated threat intelligence can further enhance detection and response capabilities by enabling timely adjustments to defense strategies based on external information.

The design of an emergency response mechanism encompasses event identification, containment of attack vectors, evidence collection and analysis, and recovery operations; key performance indicators (KPIs)—such as response time, Recovery Time Objective (RTO), and Recovery Point Objective (RPO)—must be clearly defined during the indicator-setting process. Additionally, specific response procedures should be established for different types of attacks to enhance overall security protection capabilities. Regular intrusion detection drills and evaluations should be conducted to test system effectiveness and ensure that the system can respond and handle attacks swiftly and efficiently in real-world scenarios.

4. SAFETY MANAGEMENT AND PROTECTION STRATEGIES

4.1. Safety Risk Assessment Method

Security risk assessment methods primarily consist of four core steps: asset identification, security threat analysis, security vulnerability assessment, and risk analysis and evaluation.

The asset identification phase requires a systematic review of the information systems assets—including hardware, software, data, and personnel—using both quantitative and qualitative methods to classify these assets and assign them priorities. This phase typically utilizes tools such as asset inventories and Configuration Management Database (CMDB) to identify critical assets, such as customer data, business applications, and infrastructure.

Security threat analysis focuses on both external and internal threat sources. External threats may include DDoS attacks targeting network services, malware, and social engineering; internal threats may encompass improper use or risks arising from personnel turnover. Utilizing the MITRE ATT&CK framework for threat modeling can effectively identify known attack vectors and validate their effectiveness through simulation and recovery exercises.

A security vulnerability assessment identifies known vulnerabilities in information systems using vulnerability scanning tools (such as Nessus or OpenVAS), and conducts a comprehensive evaluation by integrating these findings with periodic penetration testing and code reviews. During this phase, focus should be placed on the management of CVE identifiers and on regularly reviewing the latest risk ratings assigned to these vulnerabilities.

The core of risk analysis and assessment lies in the application of a risk assessment matrix, which assigns a risk value to each asset by determining both the likelihood of a risk occurring and its potential impact. Typically, a scoring system ranging from 1 to 5 is employed, where 1 represents low risk and 5 represents high risk. The resulting risk values should be supplemented with quantitative analysis, utilizing methods such as Fault Tree Analysis (FTA) or Event Tree Analysis (ETA), to identify and quantify potential losses.

After completing the assessment, risk response strategies should be developed, including approaches such as risk acceptance, risk transfer, risk mitigation, and risk avoidance. Among these, risk mitigation strategies are commonly employed in the implementation of security controls, such as implementing two-factor authentication (2FA), data encryption, and access control. Specific control measures should take into account implementation costs, technical feasibility, and compliance requirements.

During the risk management process, it is essential to continuously monitor and re-evaluate risk assessment results. By leveraging Security Information and Event Management (SIEM) tools, organizations can perform real-time monitoring of system status and log analysis to ensure a rapid response to potential security incidents. Additionally, the risk environment should be reviewed periodically, taking into account the impact of new technology adoption, business changes, and shifts in the external environment on the risks.

An effective risk assessment should be closely aligned with the organizations internal security policies and compliance requirements to ensure that all security measures are fully implemented, while enhancing employees security awareness through security reviews and training. This approach fosters a continuous improvement-based security management system, thereby equipping the organization with stronger risk response capabilities.

4.2. Safety Regulations and Emergency Response Procedures

The Network and Information Security Security Framework and Emergency Response section aims to establish an effective security management system that ensures rapid and efficient response to potential threats. Its core components include the formulation of security policies, assignment of responsibilities, development of incident response plans, and conduct of emergency drills.

The security policy should cover multiple aspects, including data encryption, access control, and user authentication mechanisms. Specific operational requirements include: employing the AES-256 encryption algorithm for sensitive data, with the encryption key length not being less than 256 bits;

user authentication should incorporate multi-factor authentication to ensure both the security of the login process and the authenticity of the user identity.

The responsibility allocation process must clearly define the duties pertaining to network security and information security, by appointing a Security Lead, a Technical Support Team, and an Emergency Response Team. The Security Lead shall hold certifications such as CISSP or CISM and be responsible for monitoring the implementation of security policies; the Technical Support Team shall conduct at least one network security assessment per quarter to ensure that equipment such as firewalls and Intrusion Detection Systems (IDS) is operating correctly.

The incident response plan should include steps such as incident detection, confirmation, classification, response, and recovery. Incident detection can be performed using real-time monitoring systems, such as SIEM tools, by setting thresholds for abnormal activities (e.g., a traffic spike exceeding 60%). Upon confirmation of an incident, the emergency response team shall promptly initiate a response based on classification criteria (e.g., information leakage, service denial-of-service attack, or malicious attack), ensuring that the response time does not exceed 30 minutes. During the response process, on-site forensics should be conducted, and logs should be recorded (on optical discs or SSD storage) to support subsequent investigation and analysis.

Emergency recovery strategies include the standardization of backup and recovery processes. Critical data must be backed up regularly; the backup schedule should consist of daily incremental backups and weekly full backups, with all backup data stored off-site to ensure data security in the event of a physical disaster. Additionally, the Recovery Time Objective (RTO) should be set at 4 hours, and the Recovery Point Objective (RPO) should be set at 1 hour, thereby reducing the risk of business interruption.

Regarding the monitoring and reporting mechanism, a comprehensive security incident reporting system should be established; all cybersecurity incidents, vulnerabilities, and anomalous activities must be reported within 24 hours, with detailed records of the incident occurrence time, scope of impact, and remediation measures. Regular security reports shall be issued, containing information such as incident statistics, an assessment of the effectiveness of response efforts, and recommendations for improvement, thereby ensuring transparency of information and continuous optimization of security management practices.

Emergency drills serve as a critical step in verifying the effectiveness of systems and contingency plans. Comprehensive drills should be conducted regularly—no less than once every six months—and shall include both tabletop exercises and full-scale simulations. Following each drill, it is essential to conduct a thorough summary and feedback session, analyze identified vulnerabilities, define specific improvement measures, and further enhance emergency response capabilities.

Overall, this system aims to establish an efficient mechanism for responding to cyber and information security incidents through a multi-tiered security policy framework, a clearly defined accountability system, a scientific emergency response process, and a rigorous drill system, thereby minimizing potential risks and safeguarding both information assets and business continuity.

5. CONCLUSION

In the current digital era, threats to network and information security continue to evolve, while attack methods are becoming increasingly sophisticated. To address various types of new network attacks, it is essential to adopt a multi-layered security protection strategy. Implementing a reputation model serves as an effective approach to counter malicious activities by assessing user behavior and device reputations to reduce access privileges granted to untrusted entities. For example, utilizing machine learning-based anomaly detection algorithms enables real-time identification and response to potential security threats, thereby enhancing the systems responsiveness.

Cryptography is equally vital in information security. The use of encryption algorithms such as AES (Advanced Encryption Standard) and RSA (Rivest–Shamir–Adleman) ensures the confidentiality of data during transmission. Data integrity protection can be achieved using hash functions like SHA-256 to ensure that the information has not been tampered with. Furthermore, the introduction of blockchain technology provides a novel solution for data transparency and immutability, leveraging distributed ledger technology to guarantee data security and traceability.

The deployment of network security equipment is a critical step in strengthening defense lines. Combining an IDS (Intrusion Detection System) with an IPS (Intrusion Prevention System) enables real-time monitoring and defense against malicious activities. During deployment, it is essential to focus on performance metrics such as throughput, latency, and accuracy to achieve optimal protection efficiency. Additionally, implementing vulnerability scanning tools such as Nessus or OpenVAS can help regularly identify and remediate security vulnerabilities within the system, thereby reducing the attack surface.

At the security management level, establishing robust security policies and response mechanisms is crucial. Enterprises should conduct regular security drills to test the effectiveness of their emergency response procedures and ensure that incidents can be handled promptly and effectively when a security event occurs. Additionally, conducting regular employee safety training to enhance the safety awareness and skills of all staff members constitutes a vital measure for reducing security vulnerabilities caused by human error.

With the widespread adoption of Internet of Things (IoT) devices, security policies must integrate broader device management measures. For access control of IoT devices, implementing Identity-Based Access Management (IAM) and utilizing Multi-Factor Authentication (MFA) can further enhance security. Additionally, conducting regular firmware updates and security configuration audits can effectively mitigate potential risks.

To address security protection in cloud computing environments, Security Information and Event Management (SIEM) systems are utilized to aggregate security data, enabling centralized monitoring and analysis to identify anomalous behaviors. Additionally, a hybrid cloud security strategy is implemented to ensure the encrypted storage of sensitive data, as well as to safeguard data integrity and privacy through methods such as access control and network segmentation.

To better address increasingly severe security challenges, multi-stakeholder collaboration is particularly crucial. By coordinating efforts both within the industry and with governments and research institutions, stakeholders can share security threat intelligence, respond swiftly, and continuously refine their security measures. The establishment of security alliances will facilitate the exchange and cooperation of information security technologies, pool collective strengths, and enhance overall defense capabilities.

Building a comprehensive information security ecosystem requires simultaneous advancement in both technology and management. Through continuous technological innovation, the establishment of dynamic protection mechanisms and flexible management strategies will propel network information security toward higher goals.

REFERENCES

[1] He, D. (2021). Advances in network and information security research: Special preface commemorating Mr. Xiao Guzhen. Journal of Xidian University, 6.

[2] Our journals reporter. (2021). The 9th National Cybersecurity and Information Protection Summit (XDef 2021) will be held in Wuhan. Information Security, 1, 98.

[3] Our journals reporter. (2021). The 9th National Cybersecurity and Information Protection Summit (XDef2021) was successfully held. Information Security, 1.

[4] Our journals reporter. (2021). The 9th National Cybersecurity and Information Protection Summit (XDef2021) will be held in Wuhan. Information Security, 1.

[5] Guan, Z. H. (2021). Establishment and technical exploration of computer networks and information security systems. Cybersecurity Technology and Applications, 2.

[6] Liu, F. (2021). Specific applications of blockchain technology in network and information security. Electronic Testing, 3.

[7] Wang, Y. (2021). Network information security protection measures. Papermaking Equipment and Materials, 3.

[8] Liu, Z. Y. (2021). Application of blockchain technology in network and information security. Information Recording Materials, 2.

[9] Zheng, L. (2021). Establishment and technical exploration of computer networks and information security systems. Equipment Maintenance Technology, 2.

[10] Xie, L. J. (2021). Network information security and confidentiality. Computer Procurement, 3, 28-30.

[11] Li, D. Y. (2021). Deepening network and information security supervision to support the building of a cyber power. Cybersecurity Technology and Applications, 2.

[12] Lü, Q. B. (2022). Research on network and information security risks and management systems in airports. Cybersecurity Technology and Applications, 2.

[13] Cai, L. M. (2021). Discussion on the construction of hospital network and information security systems. Cybersecurity Technology and Applications, 2.

[14] Lin, S. (2021). Key vulnerabilities in computer networks and information security and corresponding management measures. Science and Innovation, 2.

[15] Sun, Z. T. (2021). Building network and information security systems in higher education institutions — Review of Computer Network Information Security (2nd Edition). China Science and Technology Papers, 1 (Supplementary Article 7).