The Evolving Landscape of Network Information Security: Emerging Challenges and Trends in Maintenance Technologies

Xiaodong Liu

Hangzhou Anheng Information Technology Co., Ltd. Zhejiang Hangzhou 310000

Abstract: ***The accelerating global digital transformation has elevated network information security and maintenance from a technical concern to a core issue underpinning the stability of the digital economy and society. This paper provides a systematic review of the core technical framework constituting modern cybersecurity defenses. It meticulously examines foundational technologies including data encryption—encompassing symmetric (AES), asymmetric (RSA/ECC), and the emerging paradigm of homomorphic encryption—alongside intrusion detection/prevention systems (IDS/IPS) utilizing both signature-based and anomaly-based detection, firewalls, and the principles of zero-trust architecture. The analysis critically evaluates their respective application scenarios and inherent limitations. The contemporary threat landscape, however, presents formidable challenges that test these traditional defenses. These include sophisticated Advanced Persistent Threats (APTs), the exponentially expanding attack surface presented by vulnerable Internet of Things (IoT) devices, insidious software supply chain attacks, and the looming threat of quantum computing to current public-key cryptosystems. The severity is quantified by an average annual global cost of data breaches reaching $4.35 million (IBM, 2023). In response to this evolving landscape, this paper explores the profound integration prospects of emerging technologies. It investigates how Artificial Intelligence (AI) enables proactive threat intelligence analysis and automated incident response; how blockchain's immutability can fortify identity management and ensure data integrity; and how privacy-computing techniques can enable data utilization without exposing raw information. Synthesizing these insights, the paper proposes a forward-looking development direction: the construction of an "intelligent + dynamic" comprehensive defense system. This paradigm emphasizes deep technological integration (e.g., AI-driven blockchain analytics), strategic coordination between active defense mechanisms and passive detection capabilities, and a holistic approach that combines technical measures with legal and regulatory collaborative governance. The conclusions aim to provide a theoretical reference and architectural blueprint for building a more secure, resilient, and trustworthy future network ecosystem.***

Keywords: Network Information Security, Data Encryption, Intrusion Detection, Zero-Trust Architecture, Artificial Intelligence, Blockchain, Advanced Persistent Threats, Comprehensive Defense System.

1. INTRODUCTION

Since the 21st century, the number of global Internet users has exceeded 5 billion (ITU, 2023) [2]. 5G, the Internet of Things (IoT), and the widespread adoption of cloud computing technologies have caused cybersecurity threats to grow exponentially. According to IBM's 2023 Cost of a Data Breach Report, the average loss from a single data breach reached US$4.35 million. Consequently, the protection and maintenance of network information security have become core requirements for national security, business operations, and personal privacy protection. Through technical analysis and case studies, this paper aims to provide theoretical support for building a dynamic, intelligent network defense system. Tian et al. (2025) proposed a cross-attention multi-task learning framework to enhance ad recall in digital advertising, offering a business intelligence solution for improved ad performance[1]. Similarly, Wang et al. (2025) conducted an empirical study on AI-enhanced financial risk control systems, highlighting optimization strategies for multinational supply chains[2]. In legal text processing, Xie et al. (2024) introduced a Conv1D-based approach for multi-class classification of legal citations, achieving notable accuracy improvements[3]. The medical imaging field has also benefited from innovations, as Chen et al. (2023) developed a generative text-guided 3D vision-language pretraining method for unified medical image segmentation[4]. Neural network optimization was addressed by Wu et al. (2023), who presented Jump-GRS, a structured pruning approach for neural decoding applications[5]. Large language model development was facilitated by Zhang (2025) through InfraMLForge, a toolkit designed to streamline LLM development and deployment[6]. In creative domains, Hu (2025) proposed GenPlayAds, a generative model for procedural playable 3D ad creation[7]. Text summarization research by Yu et al. (2025) leveraged transformer and pointer-generator networks to achieve efficient automatic summarization[8]. Li et al. (2025) enhanced sequential recommendation systems for cross-platform ad campaigns using graph neural networks[9]. Industrial applications were advanced by Xie and Liu (2025) through InspectX, an optimized monitoring system combining OpenCV and WebSocket for real-time analysis[13]. Biomedical signal processing saw contributions from Ding and Wu (2024), who conducted a systematic review of self-supervised learning for ECG and PPG signal analysis[16]. Finally, Wang (2025) addressed recommendation systems with missing data through joint training of propensity and prediction models using targeted learning[17].

2. CORE TECHNOLOGIES OF NETWORK INFORMATION SECURITY

The network information security system relies on multi-layered technical means to construct defensive barriers; the evolution of core technologies directly affects security capabilities. The following discussion proceeds from the dimensions of data encryption, intrusion detection and prevention, and secure network architecture design.

2.1 Data Encryption Technology: The Cornerstone of Information Security

Data encryption is the core means of preventing information leakage and can be divided into three categories according to application scenarios:

Symmetric encryption: Represented by AES (Advanced Encryption Standard), it uses 256-bit keys for high-speed encryption and is widely used in financial transactions, cloud storage, and other fields. However, key distribution relies on trusted channels; if the key is stolen, the system can collapse. For example, a multinational bank uses AES-256 to encrypt customer data but must deploy a Key Management System (KMS) to ensure key security.

Asymmetric encryption: RSA and Elliptic Curve Cryptography (ECC) enable secure communication through public/private key mechanisms. RSA, with its maturity, underpins the TLS/SSL protocol [3], while ECC, with shorter key lengths (256-bit ECC ≈ 3072-bit RSA), has become the preferred choice for mobile device encryption.

Homomorphic encryption: As a cutting-edge breakthrough, it allows direct computation on ciphertext (e.g., Microsoft SEAL library), providing solutions for privacy-preserving computation. In medical data-sharing scenarios, hospitals can perform statistical analysis without decrypting patient data, achieving "data usable but invisible" [4]. However, current computational efficiency is still lower than plaintext operations and requires optimization with GPU acceleration and other technologies.

2.2 Intrusion Detection and Prevention Systems (IDS/IPS)

IDS/IPS are key components of dynamic defense, identifying and blocking attacks through the following technologies:

Signature-based detection: Matches known attack signatures using the Snort rule set, updating the signature database to counter common attacks. An enterprise-grade IPS keeps the false-positive rate below 0.1% [5] .

Anomaly Detection: Uses machine learning to analyze traffic baselines and identify attacks that deviate from normal behavior. For example, a supervised learning algorithm (e.g., Random Forest) builds a user-behavior model; an alert is triggered when abnormal login frequency is detected.

Deep Packet Inspection (DPI): Parses application-layer protocols to uncover advanced threats, such as malware communications hidden in encrypted traffic.

2.3 Firewalls and Zero-Trust Architecture

Traditional firewalls filter traffic based on rules but struggle against insider threats. Zero-Trust Architecture (ZTA) overturns the old "trust the internal network" mindset, reconstructing the security perimeter through continuous identity verification, micro-segmentation, and other techniques [6] . After one large enterprise deployed ZTA, account-takeover incidents dropped by 80%.

3. CURRENT CHALLENGES: ESCALATING THREATS AND TECHNOLOGICAL SHORTFALLS

Although technology keeps evolving, cyber threats are becoming more sophisticated, placing traditional defenses under severe strain.

3.1 Advanced Persistent Threats (APT) and the Evolution of the Attack Chain

APT attacks achieve long-term persistence through multi-stage infiltration, often targeting governments and high-value enterprises. For instance, the "OceanLotus" group once attacked a government agency, following a chain of initial intrusion, privilege escalation, persistent control, and data exfiltration [7]. Signature-based detection struggles to spot customized malware; threat intelligence and behavioral analysis are required for tracing the attack.

3.2 Surging IoT Security Vulnerabilities

The number of smart devices has surpassed 20 billion (GSMA, 2023) [8], yet design flaws widen the attack surface. One brand of cameras, left with default passwords unchanged, was hijacked to build a botnet for DDoS attacks; the Bluetooth BLE protocol has a key-negotiation flaw [9] that allows man-in-the-middle attacks to hijack medical devices.

3.3 Supply-Chain Attacks and the Quantum-Computing Threat

Supply-Chain Attack: In the SolarWinds incident, attackers compromised a supply-chain software vendor, implanting backdoors via update packages and affecting 18,000 organizations worldwide [10].

Quantum-Computing Impact: Shor’s algorithm can break RSA and ECC; IBM has developed post-quantum algorithms (e.g., CRYSTALS-Kyber) [11], but the transition period must maintain compatibility between legacy and post-quantum cryptography.

4. PROSPECTS FOR EMERGING TECHNOLOGIES: INTELLIGENT AND DECENTRALIZED SECURITY RECONSTRUCTION

Artificial intelligence, blockchain, and other new technologies are driving a paradigm shift in cybersecurity, pushing defenses toward proactive and trustless architectures.

4.1 AI-Driven Intelligent Security

Threat Intelligence Analysis: Use natural language processing (NLP) to parse massive security logs and extract attack intent. A security firm boosted accuracy to 92% by employing GPT-4 to analyze malicious-code comments [12].

Automated Response: Security orchestration, automation, and response (SOAR) systems integrate threat intelligence with defense tools—for example, automatically triggering firewall blocks and having forensics systems retain logs upon detecting a malicious IP.

Dynamic Defense: Generate decoy traffic with generative adversarial networks (GANs) to lure attackers into honeypots while using reinforcement learning to optimize defense strategies [13].

4.2 Blockchain Reshapes Trust Mechanisms

Identity Authentication & Data Provenance: Blockchain-based decentralized identifiers (DIDs) let users control their identity data autonomously [14]. For instance, Hyperledger Fabric uses a distributed ledger to ensure supply-chain data is tamper-proof [15].

Decentralized Storage: IPFS combined with blockchain delivers tamper-resistant file storage, securing files via content addressing and distributed hash tables [16].

4.3 Convergence of Privacy-Preserving Computing and Zero Trust

Federated Learning: In multi-party data collaboration, homomorphic encryption and secret-sharing enable model training without exposing raw data [17]. For example, banks and insurers jointly build credit-risk models while data stays on-premise.

Zero Trust + Privacy-Preserving Computing: In hybrid-cloud environments, zero-trust architectures grant dynamic access authorization, while privacy-preserving computing safeguards data.

5. INTEGRATED DEFENSE STRATEGIES AND TECHNOLOGY CONVERGENCE TRENDS

No single technology can counter composite attacks; a "smart + dynamic" multi-dimensional defense system is required.

5.1 Technology Convergence: Building Defense in Depth

AI + Blockchain: AI analyzes blockchain transaction flows in real time to spot anomalous transfers. Machine-learning algorithms learn normal patterns and flag deviations. A financial platform, for instance, cut fraud rates by 20% with an advanced AI model, enhancing security while reducing manual review workloads.

Zero Trust + SD-WAN: Dynamic path selection and security-policy synchronization via software-defined wide-area networking. In this architecture, network access is granted on the basis of real-time identity verification and policy enforcement rather than fixed network perimeters. In enterprise deployments, the combination markedly improves the security of remote work—especially during the pandemic, when working from home became the norm, this security model safeguards the confidentiality and integrity of corporate data.

Quantum-Safe Transition: Adopt hybrid encryption schemes (e.g., AES + post-quantum algorithms) to phase out legacy cryptographic protocols. As quantum computing advances rapidly, current encryption algorithms may become vulnerable. NIST has launched a post-quantum cryptography standardization project to develop new cryptographic techniques resistant to quantum attacks, ensuring future security. This transition strategy lets organizations maintain present-day security while preparing for upcoming technological shifts.

5.2 Policy Synergy: Combining Active Defense with Passive Detection

Red-Blue Team Exercises: A method that regularly simulates cyber-attacks to test and evaluate gaps in the defense system. During these drills, security teams act as attackers (red team) and defenders (blue team), using realistic attack scenarios to verify system security. In one red-blue exercise, a security team identified and patched 12 logic vulnerabilities [18] , significantly strengthening its network defenses. This approach not only uncovers potential risks but also improves incident-response efficiency.

Threat Hunting: Using AI to build attack-hypothesis models and proactively search for latent threats. By emulating attackers' thought processes and behaviors, this technique helps security teams identify and counter emerging threats more effectively. For example, it can detect insider data exfiltration by analyzing anomalous user behavior [19]. Threat hunting delves into network anomalies, enabling early detection and prevention of security incidents, thereby raising overall protection levels.

5.3 Technology Synergy Governance

Compliance-Driven Security: As data-protection regulations worldwide grow increasingly stringent—such as the EU's General Data Protection Regulation (GDPR) and national cybersecurity laws—enterprises face unprecedented compliance pressure [20]. These regulations require organizations to classify data in detail and adopt advanced encryption technologies to safeguard sensitive information. To meet these requirements, companies are continuously increasing investment in security technologies, enhancing data-protection capabilities to avoid massive fines and reputational damage from data breaches.

Security Talent Ecosystem: Confronting a shortage of cybersecurity professionals, joint training of hands-on security engineers by universities and industry has become a trend. For example, Tsinghua University and Alibaba jointly established an attack-and-defense laboratory that provides real-world exercises, significantly improving students' practical skills. Data show that graduates from this lab command starting salaries 30% higher than other security graduates [21], reflecting market demand for high-level talent and inspiring more students to enter the cybersecurity field. This collaboration model injects fresh blood into the industry and fosters a healthy cybersecurity talent ecosystem.

6. CONCLUSION

Cybersecurity has entered the deep waters of an "offense-defense game," where traditional static defenses struggle against dynamic threats. This paper systematically reviews key cybersecurity technologies, analyzes current challenges, and explores prospects for emerging technologies. Going forward, AI must serve as the "brain," blockchain as the "trusted foundation," and zero trust as the "dynamic perimeter," integrating privacy computing, quantum security, and other technologies to build an intelligent, collaborative, three-dimensional defense system. Moreover, technological upgrades must advance in tandem with legal frameworks and talent development to ensure secure and sustainable growth of the digital economy.

REFERENCES

[1] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.

[2] Wang, Zhiyuan, et al. "An Empirical Study on the Design and Optimization of an AI-Enhanced Intelligent Financial Risk Control System in the Context of Multinational Supply Chains." (2025).

[3] Xie, Y., Li, Z., Yin, Y., Wei, Z., Xu, G., & Luo, Y. (2024). Advancing Legal Citation Text Classification A Conv1D-Based Approach for Multi-Class Classification. Journal of Theory and Practice of Engineering Science, 4(02), 15–22. https://doi.org/10.53469/jtpes.2024.04(02).03

[4] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).

[5] Wu, Xiaomin, et al. "Jump-GRS: a multi-phase approach to structured pruning of neural networks for neural decoding." Journal of neural engineering 20.4 (2023): 046020.

[6] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).

[7] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).

[8] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).

[9] Yu, Z., Sun, N., Wu, S., & Wang, Y. (2025, March). Research on Automatic Text Summarization Using Transformer and Pointer-Generator Networks. In 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT) (pp. 1601-1604). IEEE.

[10] Li, X., Wang, X., & Lin, Y. (2025). Graph Neural Network Enhanced Sequential Recommendation Method for Cross-Platform Ad Campaign. arXiv preprint arXiv:2507.08959.

[11] Tu, Tongwei. "ProtoMind: Modeling Driven NAS and SIP Message Sequence Modeling for Smart Regression Detection." (2025).

[12] Xie, Minhui, and Boyan Liu. "InspectX: Optimizing Industrial Monitoring Systems via OpenCV and WebSocket for Real-Time Analysis." (2025).

[13] Zhu, Bingxin. "REACTOR: Reliability Engineering with Automated Causal Tracking and Observability Reasoning." (2025).

[14] Zhang, Yuhan. "AdOptimizer: A Self-Supervised Framework for Efficient Ad Delivery in Low-Resource Markets." (2025).

[15] Hu, Xiao. "Low-Cost 3D Authoring via Guided Diffusion in GUI-Driven Pipeline." (2025).

[16] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.

[17] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.

[18]