Exploration of Security Vulnerabilities and Encryption Technologies for Computer Information Technology Data

Zhouping Lu

Greentown Technology Industry Service Group Co., Ltd., Hangzhou 310000, Zhejiang, China

Abstract: ***The transmission, use, and storage of computer information technology data face various security vulnerabilities, exposing data to risks such as theft and destruction. As a key means of protecting computer information technology data, data encryption technology can maximize the effectiveness of vulnerability protection. Based on actual conditions, this paper first analyzes the factors influencing computer information data security vulnerabilities, then elaborates on the main forms of such vulnerabilities in computer information technology data, and finally proposes targeted applications of data encryption technology in computer information technology for reference.***

Keywords: Computer information technology data; Security vulnerabilities; Encryption technology.

1. INTRODUCTION

The rapid development of information technology has profoundly influenced the operation and production models of all sectors of society; computer information technology has penetrated every aspect of social life. Users face numerous data security risks when utilizing computer information technology data, especially various data security vulnerabilities that expose network data to threats of illegal access, theft, and leakage. If data is stolen or lost, users may suffer severe losses. Aligning with the types of security vulnerabilities in computer information technology data, employing various encryption technologies has become an important means of enhancing data security. The use of encryption technology can maximize the security of computer information technology data and plays a vital role in creating a secure network application environment. Chen et al. (2024) introduced Bimcv-r, a landmark dataset tailored for 3D CT text-image retrieval, providing a valuable resource for medical image analysis [1]. In the realm of natural language processing, Yu et al. (2025) explored automatic text summarization using Transformer and Pointer-Generator Networks, demonstrating promising results in information condensation [2]. Sun et al. (2025) focused on constructing an Automated Machine Learning (AutoML) framework based on large language models, aiming to streamline the machine learning pipeline [3]. Pal et al. (2025) proposed an AI-based credit risk assessment and intelligent matching mechanism in supply chain finance, enhancing financial decision-making processes [4]. Wang and Zhao (2024) advanced abstract reasoning in artificial general intelligence by introducing a hybrid multi-component architecture [5]. In the area of large language model robustness, Fu et al. (2025) presented Adversarial Prompt Optimization in LLMs, highlighting the importance of robustness and defense evasion strategies [6]. Lei et al. (2025) developed a Teacher-Student Framework for short-context classification, incorporating domain adaptation and data augmentation techniques to improve model generalization [7]. Zheng et al. (2025) introduced FinGPT-Agent, an advanced framework for multimodal research report generation, featuring task-adaptive optimization and hierarchical attention mechanisms [8]. Weng et al. (2025) proposed SafeGen-X, a comprehensive framework aimed at enhancing security, compliance, and robustness in large language models [9]. Chen et al. (2025) introduced SyntheClean, a method for enhancing large-scale multimodal models through adaptive data synthesis and cleaning [10]. Jiang et al. (2025) developed a knowledge-enhanced multi-task learning model for domain-specific question answering, demonstrating the effectiveness of integrating external knowledge sources [11]. Zhuo et al. (2025) proposed an intelligent-aware Transformer with domain adaptation and contextual reasoning capabilities for question answering tasks [12]. Zhang et al. (2025) explored dynamic attention-guided video generation from text, utilizing multi-scale synthesis and LoRA optimization techniques [13]. Zhao et al. (2025) introduced KET-GPT, a modular framework for precision knowledge updates in pretrained language models [14]. Shih et al. (2025) developed DST-GFN, a dual-stage Transformer network with gated fusion for pairwise user preference prediction in dialogue systems [15]. Li et al. (2025) proposed MLIF-Net, a multimodal fusion approach combining vision transformers and large language models for AI image detection [16]. In biomedical signal processing, Ding and Wu (2024) conducted a systematic review on self-supervised learning for ECG and PPG signals, providing insights into the current state-of-the-art [17]. Restrepo et al. (2024) explored multimodal deep learning for low-resource settings, proposing

a vector embedding alignment approach for healthcare applications [18]. Xie and Chen (2025) introduced CoreViz, a context-aware reasoning and visualization engine for business intelligence dashboards, enhancing data interpretation capabilities [19]. Zhu (2025) proposed TraceLM, a temporal root-cause analysis framework utilizing contextual embedding language models [20]. Zhang (2025) developed InfraMLForge, a developer tooling for rapid LLM development and scalable deployment [21]. Another work by Zhang (2025) introduced SafeServe, a scalable tooling for release safety and push testing in multi-app monetization platforms [22]. Hu (2025) explored procedural playable 3D ad creation via generative models in GenPlayAds [23] and immersive 3D ad content creation via game engine pipelines in UnrealAdBlend [24]. Finally, Wang (2025) investigated joint training of propensity and prediction models via targeted learning for recommendation systems dealing with data missing not at random [25]. These studies collectively contribute to the advancement of AI technologies across various domains, highlighting the diversity and depth of current research efforts.

2. FACTORS INFLUENCING COMPUTER INFORMATION DATA SECURITY VULNERABILITIES

2.1 Human Factors

The rapid development and widespread adoption of information technology have continuously raised the level of computer automation, yet using computer equipment still requires human input of operational commands to control the devices. During use, the operator's own application skills and security awareness, along with the standardization of data usage, directly affect the effectiveness of computer information technology data security. Currently, common computer attack methods include computer viruses; virus intrusion usually occurs when operators fail to notice abnormal data while executing programs, allowing malicious code to mix with normal data and flow into the computer system, resulting in viral damage. Many viruses have an incubation period and show no immediate effect, but spread rapidly at a specific moment [1]. The implantation of these viruses can lead to the complete leakage and destruction of data collected by the computer, creating clearly visible security vulnerabilities.

2.2 Other Factors

In addition to human factors, the emergence of data security vulnerabilities in computer information technology also involves other elements. For example, security flaws inherent in installed computer programs can likewise allow virus intrusion. Compared with vulnerabilities caused by human factors, those rooted in the operating system itself are more concealed, harder to trace, and take diverse forms. If not repaired promptly, they will further intensify the spread of the vulnerability. Data security flaws arising from non-human factors are directly related to the development and programming of computer programs. Problems in the execution or coding of the code involved in development generate security vulnerabilities, undermining the secure use and storage of information.

3. MAIN FORMS OF DATA SECURITY VULNERABILITIES IN COMPUTER INFORMATION TECHNOLOGY

3.1 Web Link Security Vulnerabilities

The rapid development and widespread adoption of information technology have profoundly transformed production and operational models across all sectors of society. In the information age, data has become a new class of assets. As computer information technology continues to permeate every level of society, the public has become increasingly dependent on it, using it more extensively, and it has become a fundamental technology essential to the production of many enterprises. During the use of computer information technology, some users have weak security awareness, lack a correct understanding of security vulnerabilities, possess insufficient knowledge of data leakage issues, and are short of proper preventive measures, leading to the emergence of web-link security vulnerabilities. A web-link security vulnerability is a disguised form of flaw that conceals malware within a hyperlink. Some users, when operating computers, fail to guard against unfamiliar links; once they click such links, viruses infiltrate, resulting in information theft and personal data exposure. Web-link security vulnerabilities are relatively common, and users must remain vigilant against unfamiliar links to prevent virus intrusion. Moreover, enterprises store large volumes of production data and product information on their computer equipment; these data assets are critical to the business. If staff members click on unfamiliar links while using the equipment, allowing viruses to penetrate the database and locate where corporate data are stored, the enterprise

risks data loss, corruption, or tampering, potentially incurring enormous economic losses.

3.2 Hacker Intrusion Security Vulnerabilities

Hacker intrusion security vulnerabilities primarily manifest as hacker attacks. Many malicious actors exploit security flaws in computer systems to break in and obtain user information and data. High-frequency attacks can even breach firewalls, posing a severe threat to the security of computer information technology. It can be said that hacker intrusion vulnerabilities are the most widespread and among the most destructive forms of security flaws in computer information technology. Hackers employ diverse methods with formidable destructive power, leveraging system vulnerabilities to compromise systems, forcibly acquire users' personal information, and even manipulate systems to alter data. Because hacker intrusion techniques are so varied, ordinary users cannot accurately identify attack vectors; personal data may be stolen in ways that go unnoticed, creating significant security risks for the use of computer information technology.

3.3 Trojan Horse Security Vulnerabilities

During operation, computer equipment relies on various types of software to store, use, and retrieve information. Security vulnerabilities in software constitute a major hidden danger. Flaws in systems and software are the prerequisite for Trojan horse viruses to intrude, and the continuous spread of these vulnerabilities can easily trigger the risk of data leakage. In computer information technology, software security vulnerabilities are mainly manifested in two aspects: virus intrusion and illegal attacks. Trojan horse viruses not only spawn a large number of network viruses, but also make virus tracing significantly more difficult. They propagate extremely fast, are highly destructive, and exert a strong impact on computer network security systems. Damage of varying degrees caused by Trojan horse attacks will directly expose users' personal data to the risks of leakage and destruction [2]. Advanced Trojan horse programs can even take control of the user's computer and alter software program instructions, collecting all data information used on the computer. Users who lack computer security awareness and technical skills have poor ability to identify and block Trojan horse viruses.

3.4 Firewall Security Vulnerabilities

A firewall is an important security protection system in computer information systems, playing a key role in blocking viruses and hacker attacks. However, in practice, the security level and protection strength of a firewall are directly related to its technical sophistication. Some users lack sufficient security awareness and do not attach great importance to firewall usage. In addition, certain firewalls themselves have low protection levels and weak defense capabilities, allowing viruses to exploit firewall security vulnerabilities to collect data without the user noticing. Many users have a shallow understanding of firewalls; while relying too heavily on firewall alerts, they use low-grade firewalls and find it difficult to grasp the security vulnerabilities that exist, making firewall vulnerability management highly challenging.

4. APPLICATION OF DATA ENCRYPTION TECHNOLOGY IN COMPUTER INFORMATION TECHNOLOGY

4.1 Application of Virtual Private Networks

A Virtual Private Network (VPN) is a virtual private network built on data-encryption technology, primarily applied to computer information security through remote access, enterprise networking, and anonymous browsing. While operating, a VPN establishes an encrypted data-transmission tunnel over the open public Internet; any data passing through this tunnel must undergo encryption verification, and data that fails verification cannot enter the device. The encryption algorithm used by VPN technology is a hybrid scheme that combines asymmetric and symmetric encryption. This combination effectively reduces the security threats posed by the open Internet, delivering stronger encryption and higher data-transmission efficiency. Symmetric encryption uses a shared key to secure data within the VPN tunnel; it is characterized by high efficiency and fast speed, meeting the performance demands of large-scale data transmission. However, because the key is shared one-to-one, key management and distribution are difficult—every user who needs the data must obtain the key. Therefore, integrating asymmetric encryption with symmetric encryption allows secure key exchange over the VPN encrypted channel while still enabling large-scale encrypted data transmission.

Enterprises and institutions are the primary use cases for VPN technology. In particular, organizations with

cross-regional operations can leverage VPN's point-to-point encryption to interconnect branch offices in different regions, creating a high-quality enterprise private network that supports business operations. This fully encrypted network enables secure communication between headquarters and branches, as well as between branches themselves. Headquarters and branch employees need only connect to the VPN encrypted tunnel to efficiently and securely access the corporate intranet and achieve high-speed data interaction and application [3]. Everyday users can also enhance their security by setting up a VPN, especially when transmitting data over unfamiliar networks; by hiding their IP address, they can avoid network tracking, laying the foundation for secure and efficient transmission of personal information and data.

4.2 Application of the Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure (HTTPS) is the most widely used encryption technology with the broadest scope of security protection; it is a secure communication protocol commonly employed in web applications. HTTPS primarily inserts a Secure Sockets Layer between the application-layer HTTP protocol and the transport-layer TCP protocol in computer networks, so all data flowing from the application layer to the transport layer must have its integrity verified and its identity authenticated. The hybrid encryption mechanism adopted by HTTPS is highly flexible, ensuring data security while maintaining efficient information transfer. Once an HTTPS connection is established, the SSL/TLS handshake is triggered; this is an interactive process between the sender and the receiver. During the handshake, subsequent communication uses a symmetric encryption algorithm for key exchange, effectively solving the difficult problem of key sharing in asymmetric algorithms. Asymmetric encryption involves high computational overhead and slower data transmission, but it offers greater security and is therefore widely used for transmitting confidential or critical files. In asymmetric encryption, the client uses a public key, while the private server must use a private key to decrypt the data; even if the data is intercepted by malicious actors, the information cannot be decrypted without the private key. After key exchange, HTTPS encrypts data transmission by combining symmetric encryption with private-key techniques, enabling large-scale data encryption.

Meanwhile, HTTPS has also introduced digital certificate technology, laying the foundation for identity authentication between both parties in data transmission. At present, the PKI system for digital certificates is relatively flexible, covering information such as the scope of certificate authentication, the digital signature of certificate issuance, server domain names, and private server keys. During the use of digital certificate technology, it is necessary to verify the server domain name and the server's encryption public key in the data flow to prevent attacks such as DNS hijacking and virus intrusion [4]. HTTPS offers significant advantages in computational performance, but it also increases cost overhead for computer users in terms of communication latency and encryption computation, especially since the SSL/TLS handshake process requires the use of asymmetric and symmetric encryption algorithms, with encryption, decryption, and certificate verification consuming higher time and computational costs. As computer hardware devices are upgraded through different stages, the time required for the SSL/TLS handshake process continues to decrease. At the same time, thanks to performance optimizations in HTTPS, performance losses during certificate verification and encrypted data transmission have been further reduced, greatly enhancing overall security and maturity. Currently, HTTPS has become the standard encryption technology used by enterprises and institutions in web applications; software such as online banking, corporate email, and social media have all begun to adopt HTTPS on a large scale for encryption, playing an important and positive role in protecting the secure transmission of private and confidential data and curbing cyber threats. At present, the next-generation HTTPS/3 standard has become a key direction for web network security encryption. In the future, HTTPS is also expected to break through the limitations of the web network, providing encryption support for more network application scenarios such as the industrial internet and the internet of things, laying the foundation for achieving the goal of "interconnection of all things."

4.3 Application of Blockchain Technology

Blockchain, originally devised as the underlying algorithm for Bitcoin mining, was not initially applied to network security encryption. With the continuous advancement of information technology and the growing ubiquity of networks, blockchain's advantages—such as chain-of-blocks storage, immutability, and secure, trustworthy decentralization—have quickly turned it into a global technology widely adopted for data encryption in computer information systems. By leveraging cryptographic principles, blockchain establishes a technical framework for maintaining data trustworthiness. Its ability to guarantee strict data immutability stems from a suite of cryptographic techniques, including hash algorithms, asymmetric encryption, consensus algorithms, and elliptic-curve digital signatures. Compared with other encryption technologies, blockchain integrates a broader

array of algorithmic logic and technical methods, skillfully combining cryptography, consensus mechanisms, and distributed storage to ensure data integrity at its core [5]. Currently, blockchain is in a phase of rapid development; it still faces numerous challenges in large-scale cryptographic adoption, privacy protection, and technical regulation, and achieving widespread commercial deployment requires overcoming a series of technical hurdles. Nevertheless, as a novel cryptographic application, blockchain has become a key direction for data encryption in computer information technology, providing comprehensive data support for Internet infrastructure and offering valuable innovation for highly confidential data transmission and the construction of tamper-proof trust in computer information systems.

5. CONCLUSION

In summary, the rapid development and widespread adoption of information technology have profoundly influenced every sector of society. At present, the use and storage of data in computer information systems suffer from a range of security vulnerabilities that pose serious threats to data security. Employing a variety of data encryption technologies is a crucial method and technical foundation for safeguarding data in computer information systems; only through rational and efficient application of these encryption technologies can we build a robust and solid network security defense. Aligning with the characteristics of the new era and keeping pace with evolving cybersecurity landscapes, we must judiciously apply encryption technologies to create a more efficient and harmonious network application environment.

REFERENCES

[1] Chen, Yinda, et al. "Bimcv-r: A landmark dataset for 3d ct text-image retrieval." International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2024.
[2] 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.
[3] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.
[4] Pal, P. et al. 2025. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. Journal of Theory and Practice in Economics and Management. 2, 3 (May 2025), 1–9.
[5] Wang, Yang, and Zhejun Zhao. "Advancing Abstract Reasoning in Artificial General Intelligence with a Hybrid Multi-Component Architecture." 2024 4th International Symposium on Artificial Intelligence and Intelligent Manufacturing (AIIM). IEEE, 2024.
[6] Fu, Lei, et al. "Adversarial Prompt Optimization in LLMs: HijackNet's Approach to Robustness and Defense Evasion." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.
[7] Lei, Fu, et al. "Teacher-Student Framework for Short-Context Classification with Domain Adaptation and Data Augmentation." (2025).
[8] Zheng, Haoran, et al. "FinGPT-Agent: An Advanced Framework for Multimodal Research Report Generation with Task-Adaptive Optimization and Hierarchical Attention." (2025).
[9] Weng, Yijie, et al. "SafeGen-X: A Comprehensive Framework for Enhancing Security, Compliance, and Robustness in Large Language Models." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[10] Chen, Yang, et al. "SyntheClean: Enhancing Large-Scale Multimodal Models via Adaptive Data Synthesis and Cleaning." 2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA). IEEE, 2025.
[11] Jiang, Gaozhe, et al. "A Knowledge-Enhanced Multi-Task Learning Model for Domain-Specific Question Answering." 2025 7th International Conference on Information Science, Electrical and Automation Engineering (ISEAE). IEEE, 2025.
[12] Zhuo, Jiayang, et al. "An Intelligent-Aware Transformer with Domain Adaptation and Contextual Reasoning for Question Answering." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[13] Zhang, Hanlu, et al. "Dynamic Attention-Guided Video Generation from Text with Multi-Scale Synthesis and LoRA Optimization." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.

[14] Zhao, Shihao, et al. "KET-GPT: A Modular Framework for Precision Knowledge Updates in Pretrained Language Models." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[15] Shih, Kowei, et al. "DST-GFN: A Dual-Stage Transformer Network with Gated Fusion for Pairwise User Preference Prediction in Dialogue Systems." 2025 8th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). IEEE, 2025.
[16] Li, Xuan, et al. "MLIF-Net: Multimodal Fusion of Vision Transformers and Large Language Models for AI Image Detection." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[17] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.
[18] D. Restrepo, C. Wu, S.A. Cajas, L.F. Nakayama, L.A. Celi, D.M. López. Multimodal deep learning for low-resource settings: A vector embedding alignment approach for healthcare applications. (2024), 10.1101/2024.06.03.24308401
[19] Xie, Minhui, and Shujian Chen. "CoreViz: Context-Aware Reasoning and Visualization Engine for Business Intelligence Dashboards." Authorea Preprints (2025).
[20] Zhu, Bingxin. "TraceLM: Temporal Root-Cause Analysis with Contextual Embedding Language Models." (2025).
[21] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).
[22] Zhang, Yuhan. "SafeServe: Scalable Tooling for Release Safety and Push Testing in Multi-App Monetization Platforms." (2025).
[23] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).
[24] Hu, Xiao. "UnrealAdBlend: Immersive 3D Ad Content Creation via Game Engine Pipelines." (2025).
[25] 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.