World Journal of Innovation and Modern Technology, Vol. 8, Issue 8 (Aug) 2025
ISSN 2682-5910
DOI: 10.53469/wjimt.2025.08(08).03

Application of Data Encryption Technology in Computer Network Information Security

Mingxiaofan Liu

No. 164 Hanghe Street, Urban Area of Yucheng, Shandong province Yucheng 251200

Abstract: ***In recent years, in the context of the rapid development of computer network information technology in China, network systems have formed interoperability mechanisms. However, this situation can also cause networks to become disaster areas for information leaks. This requires the integration of computer information. Through the effective application of data encryption technology, security risks can be found in time, so as to provide conditions for the stable operation of computers.***

Keywords: Computer; Network information security; Data encryption technique.

1. INTRODUCTION

At present, in order to achieve the safe transmission of information in the information age, it is necessary to strengthen the effective application of data encryption technology. In the computer information system, realize the integration of data information, shorten the distance of time and space, ensure the security of network operation, eliminate the security problems of network information transmission in time, and then realize the encryption of key data information. 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. CHARACTERISTICS OF DATA ENCRYPTION

At present, in order to ensure the validity of computer data encryption technology in network information transmission, its principle is analyzed. It mainly allows the sent information data to become meaningful ciphertext by integrating and encrypting the relevant data information, implementing the transformation between functions, on this basis. After receiving the key, we can use scientific methods to comprehensively interpret the translation, so that it can be restored to the original data [1].

In the application of data encryption, it is necessary to ensure that it has specific requirements, to strengthen its effective use in a specific environment, to achieve rapid conversion of the original content. The key is the main part of data encryption. Through the key, technicians can convert the key to the source file more flexibly.

3. FACTORS AFFECTING COMPUTER NETWORK SECURITY

3.1 Risks in information operating systems

The core software of a computer is the operating system. However, the computer operating system still has some problems in operation, and if the operating system is affected by viruses, it will cause problems in the overall computer operation. Viruses can directly obtain the user's password, making it very easy to manipulate the overall system and obtain user information in all programs on that basis. In general, the virus will also monitor the transmission and use of users' information through spyware programs, which will cause the overall server to become paralyzed. In addition, the virus intruders can also use the weak links in the information system, such as remote call function and other vulnerabilities, to achieve the computer system of the infringement, seriously affecting the security of information transmission [2].

3.2 Security Risks in Database Management Systems

Often, some database management systems cause problems in operation, and if they are not processed in a timely manner, it will affect basic information such as bank card passwords or personal identity cards. These security issues will pass through the database, and if it is not highly secured, it will be exposed to the outside world. This moment virus invader can pass information base, undertake using to user information, achieve the purpose that destroys computer then.

3.3 Security in the network

Although the emergence and development of the Internet can make human life more enriching and convenient. However, there will be information security issues in operation, there are relatively large security risks. It is mainly from the destruction of transmission lines, or network protocols affected, etc., will bring a very big impact on computer software and hardware. In addition, these unsafe factors, but also on the user's information security impact. Therefore, it is necessary to start from the characteristics of computer system, through the effective application of data encryption technology, to avoid its impact on the firewall [3].

4. DATA ENCRYPTION TECHNOLOGY IN THE COMPUTER NETWORK INFORMATION SECURITY

4.1 Cryptography

If we analyze the use and characteristics of data encryption in cryptography, the encryption device has been invented in the 5th century BC. At that time, parchment was the carrier of information, and without the guidance of external objects such as wooden sticks, we could not effectively read the text in time, which required wrapping the parchment around the corresponding wooden stick to achieve the decoding of the text.

Therefore, it is necessary to strengthen the in-depth study of cryptography, make clear the characteristics of encoding and decoding, and perfect and innovate the data encryption technology based on mathematics, geometry and information technology. In the 21st century, in order to achieve the integration of social data information, AES, a new data encryption standard, needs to be integrated. In cryptology, strengthen the effective application of data encryption technology, from the point of view, to achieve information data security, so as to provide conditions for the safe operation of the network system.

4.2 Classic encryption algorithms

First of all, DES. This classical symmetry is also known as encryption algorithm, some countries have it as the data encryption standards, belongs to a symmetric encryption and decryption algorithm. At the same time, the DES algorithm can also encrypt information data in the encryption mode in combination with the default key. In decryption mode, technicians can use the key to decrypt it, not knowing that the keyholder is very difficult to decipher the information in it, and cannot consolidate and encrypt a large amount of information data in a short period of time.However, DES encryption and decryption will use the same key, so after knowing the encryption key, you can complete the decryption, so the security of this method is not high [4].

Then there's MD5. MD5 message this algorithm is also called 128-bit encryption algorithm, generally used in information detection, belongs to an irreversible encryption technology. Therefore, this technology has been effectively used in user login passwords. This algorithm can be arbitrary length and character strings to convert, this conversion is not reversible. However, when analyzing the data encryption technique, the scholars found that

because of the illogical conversion between the characters, it can not decipher the related data into the original data.

Some scholars found that the MD5 algorithm does not require the length of the plaintext, but the output ciphertext has a fixed 128 bits, which has some limitations in the application of network data encryption, and the overall practicality is not high. Finally, the RSA algorithm. This method has developed into a perfect RSA system in the later period. This algorithm solves the problem of prime numbers through the multiplication of two large prime numbers, mainly using the multiplication and so on as the public key, strengthening the analysis of the algorithmic results, and using it as the private key, on this basis, achieves the encryption of relevant information.

However, the private key can only be mastered by legitimate persons, and in theory, the private keys can be analyzed for data information through the multiplication of public key primes. However, this amount of computing is very large and is a very highly secure form of encryption.

4.3 Strengthening the defensive effect of firewalls

In the operation of the computer network system, to achieve the security protection of information, the firewall should actively play the role in it. It is mainly to achieve the maintenance of network security and strengthen the protection of computer network security. Normally, computers have a firewall during operation, which has the effect of detecting hazards. If a user visits some web pages or downloads other data, they check the security of the web pages and data. When it detects network security risks, it will prompt users in time [5].

Therefore, the related technical personnel need to strengthen the effective application of data encryption technology, the establishment of firewall, scientific application of computer technology, to ensure the security of computer network system. At the same time, it can also help users achieve comprehensive defense against network risks on the basis of this firewall. In the process of applying a firewall, it is also possible to use a server on this basis, Constructing security platform to integrate all kinds of data in the computer to realize the comprehensive detection and scanning of the relevant information, and to deal with the security problems existing in the operation of the computer in time to provide conditions for the safe operation of the network information system.

4.4 Enhancing the functionality of computer software

At present, with the effective application of computer technology in various fields of social development, relevant technicians have strengthened the software functions in network systems. At the same time, we also need to take measures to do a good job of encryption and protection of computer software to ensure the effective application of data encryption technology in specific information protection. If the user does not enter the correct key in the computer network when applying it, or if the user has entered it multiple times incorrectly, the software will not function more normally and steadily.

This needs to play a positive role in the protection of computer systems, timely detection of malicious viruses, and then the scientific application of data encryption technology to improve computer systems, reduce its attack by other factors. In addition, we must implement the installation of defensive software, promptly remind users to eliminate viruses regularly, and achieve comprehensive defense against viruses. If virus traces are found in the application of computer systems, they should be processed in a timely manner, thereby continuously strengthening the security of computer network operation.

4.5 Strengthening the Application of Data Encryption Technology in Local Area Network

The study found that if information technology is applied and a local area network is set up, it can not only achieve the transmission of information between information, but also the integration of data information. Especially in the use of a local area network, to further ensure the stability and security of information transmission, the information data, etc., must be strictly encrypted, so that the data can be automatically stored in the router during transmission. If it is transmitted to other routers, it can be automatically decrypted [6].

In addition, to strengthen the effective application of data encryption technology in the LAN, but also to ensure that information recipients can directly access their own information. At the same time, it is necessary to strengthen the scientific use of various data encryption methods, mainly in order to prevent information disclosure,

to ensure the safety of information data, to promote the effective transmission of information for the safe operation of the Internet information system.

5. CONCLUSIONS

In short, the previous computer information encryption technology can no longer meet the requirements of social development. In order to ensure the security of the current network information transmission, it is necessary to strengthen the effective application of data encryption technology from different angles. At the same time, through the analysis of data encryption algorithm, we can promote the transmission of data information, strengthen the protection of user information, and avoid information leakage in the operation of computer systems.

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.