Application of Cryptography Technology Based on Network Information Security

Yunyu Cao

School of IoT Engineering, Wuxi University 214105

Absrtact: ***The rapid progress of science and technology has promoted the increasingly serious challenges to Internet security, such as virus intrusion, hacker attacks and data leakage.In order to address these issues, the development and use of cryptography have emerged, whose functions include maintaining the stability of computer systems to prevent data counterfeiting or modification, while ensuring the confidentiality and integrity of data within the system.This article mainly elaborates on the importance of information security in the current society, and provides a detailed introduction to cryptographic technology, especially exploring the practical application of cryptographic technology in the field of network information security for reference by colleagues.***

Keywords: Cryptography technology; Network information security; Computer network.

1. INTRODUCTION

As early as in ancient times, cryptographic technology has begun to be widely used in protecting information security in key areas such as diplomacy and military affairs. Now, due to the rapid progress of Internet technology, it is gradually penetrating into various industries.In addition to ensuring the strict confidentiality of confidential data on computer networks, password technology is also applicable to digital signatures, network system security, and other aspects.By utilizing the principles of cryptography, we can maintain the consistency and immutability of network information while ensuring its security and privacy.In addition, this also helps prevent the risk of unauthorized modification or forgery of personal data. Diao et al. (2025)[1] made notable progress by optimizing Bi-LSTM networks to enhance lung cancer detection accuracy, achieving improved diagnostic performance through deep learning techniques. Urban analytics has benefited from Li et al. (2025)[2]'s innovative work on interactive data exploration for smart cities, which introduced a user-centered perspective to urban data analysis. Complementing this, Wang (2025)[3] developed AI-driven solutions for smart city logistics, specifically focusing on optimizing last-mile delivery efficiency through intelligent routing algorithms. In computer vision and security applications, Bohang et al. (2025)[4] advanced the field of image steganalysis by implementing active learning combined with hyperparameter optimization, demonstrating superior detection capabilities. Industrial applications have seen substantial improvements through AI integration, as evidenced by Zhao et al. (2024)[5]'s deep learning approach to steel production scheduling optimization, which significantly enhanced manufacturing efficiency. Economic forecasting has similarly benefited from AI, with Yang et al. (2025)[6] developing a novel big data-based method for economic cycle prediction that outperforms traditional models. Healthcare infrastructure has been transformed by Xu (2025)[7]'s application of graph convolutional networks (GCNs) to optimize healthcare facility design, achieving both structural and functional improvements. The financial sector has embraced AI through Jiang et al. (2025)[8]'s Investment Advisory Robotics 2.0 system, which leverages deep neural networks to provide personalized financial guidance with unprecedented accuracy. Network optimization has progressed through Tu (2025)[9]'s Log2Learn framework, which employs intelligent log analysis for real-time network performance enhancement, demonstrating the versatility of AI across technical domains.

2. THE IMPORTANCE OF NETWORK INFORMATION SECURITY

Although there have been discussions about online information in earlier years, its importance has not received sufficient attention.However, with the development and wide application of the Internet, communication protection has gradually become the focus of public attention.Now, we have fully recognized the significant importance of network information security, which not only concerns social stability, wealth security, and personal life stability, but may also lead to issues such as hacker attacks, electronic espionage activities, computer crimes, data loss, network protocols, and information wars.These issues not only affect our work and life, but also have a huge impact on national security, military strength, international relations, and even the operation of government institutions.At present, the functions of network information systems have become a core part of a country's economic development, political decision-making, cultural and social activities. If they are damaged and cannot operate, it will cause huge losses to the entire country, such as weakened military combat effectiveness, interrupted communication lines, paralyzed financial systems, and so on. In the worst case, it may trigger domestic economic crises, political instability, and social disorder, with unpredictable consequences.In summary, our passwords in daily life are facing severe challenges, especially from a risk known as' collective threat ', which is like spam and does not directly target individuals.Not all hackers only focus on cracking individual accounts, they are completely unaware of personal information, and their goal is simply to collect a list of cracked account passwords and sell them for profit.People who steal secrets will choose to use cracking software, starting with websites with lower levels of security protection.After these software are successfully guessed, they will use the same secret and its variants to attack more secure and reliable accounts, such as bank accounts.Therefore, research on cryptography has extremely high value and significance [1].

3. INTRODUCTION TO CRYPTOGRAPHY TECHNOLOGY

Cryptography technology is one of the core guarantee measures for computer network information security, which mainly uses the encryption and decryption process of key information within the network to protect its integrity and confidentiality.Only authenticated or authorized users are allowed to enter the network system.The main purpose of this technology is to ensure the security of sensitive data and important information on computers.

3.1 Cryptography and its Applications in Network Information Security

As a methodology for designing secure systems based on computing devices, cryptography research originated from its construction and parsing process.It not only provides highly conservative data protection measures for government agencies in various countries, but also becomes one of the key means of safeguarding the privacy of commercial companies and individuals.We can see its existence and play a role in everything from banks to the military to international business transaction venues.With the progress of society and changes in lifestyle, people's digital lives are increasingly inseparable from this tool.The Internet architecture depends entirely on this mechanism to determine the true identity of users.Once these secrets are exposed or tampered with, they may lead to unpredictable and serious impacts on this globally interconnected network connected by computers.So in order to ensure that personal information is not infringed upon or exploited by attackers, effective protective strategies must be taken to prevent such situations from happening.The most commonly used and secure method so far is to strictly review and process all transmitted information content through various advanced technologies such as code generators and substantive detection programs.At the same time, suitable powerful, reliable, and easy-to-use high-performance cryptographic operation models and their corresponding mathematical formula combination schemes will be selected according to the needs, in order to better ensure the integrity and authenticity of information without any form of external interference, thus achieving the best results.So, these actions that may lead to computer network information security can be interdependent or adversarial, which helps promote the progress and development of cryptography.

At present, cryptographic techniques used in computer networks can be divided into two categories: one is based on mathematical applications, including key management, virtual private network (VPN) technology, and digital signatures;The other type is not based on mathematical application technology, such as biometric based identity authentication technology and quantum encryption.In order to ensure the information security of computer networks, we must make reasonable use of these cryptographic techniques to construct effective computer network information security systems.

3.2 Private Key Cryptography Techniques

In the Internet environment, the application of private key cryptography has a long history. It allows two participants to share the same password to encrypt or decrypt data and information.The task of each participant is to use this password to perform the corresponding encryption or decryption actions.Due to the fact that only the same key can be used for these two processes, the entire process becomes more concise and clear.As long as the private key is not disclosed by any party, the security and integrity of the message content can be ensured.

3.3 Public Key Cryptography Techniques

As a commonly used encryption method, computer public key encoding technique is also known as asymmetric code strategy.Each user has their own numerical correlation, namely a public key and a private key. Although these two different solutions are generated by a pair, only by mastering either set can the information content of the other party be decrypted.This technology can not only ensure the security and confidentiality of personal information on the Internet, but also enhance the credibility of the network communication system.This science can enable people on both ends of the Internet to communicate safely without first sharing their personal identification numbers;At the same time, it can also be used in various important situations such as customer verification, etc. [2].

4. THREATS TO COMPUTER NETWORK SECURITY

4.1 Unauthorized Access

Private use of network resources without prior permission of individuals or Internet managers will be deemed as unauthorized access. This type of infringement includes intentional avoidance of computer network monitoring systems, access restriction systems, improper use of computer network resources and other violations, and may even exceed their due rights to obtain computer network data.The main forms of unauthorized access include disguised or illegal login operations to specific systems, or unauthorized operations by legitimate logins.

4.2 Loss or leakage of computer information

Information loss or leakage refers to the unintentional or intentional leakage of sensitive data in computer networks, such as network hackers eavesdropping or electromagnetic leakage of confidential data, resulting in the loss of important computer information.

4.3 Characteristics of Disrupting the Integrity of Computer Network Data

Once unauthorized information is stolen on a computer network, the act of adding or changing critical information is aimed at eliciting a positive response from hackers.By altering or adding elements of the original information to disrupt the normal and reasonable operations of computer network users.

4.4 Interference with Service Systems

In the computer network environment, various potential risks and dangers can have a sustained impact on the computer network service system, forcing it to adjust its normal operation mode to run non essential software or reduce its response speed to network services, which may ultimately lead to the collapse of the entire service system.So, those normal computer network users cannot access the computer network smoothly and enjoy the corresponding services.

5. THE PRACTICAL APPLICATION OF CRYPTOGRAPHY IN NETWORK INFORMATION SECURITY

5.1 Plays a role in encryption protection

As the core part of cryptography, the function of password transformation is to reasonably convert the original text into ciphertext that only authorized users can understand.This process involves two main types: encryption during message transmission;The second is the encryption of stored information.

For the first scenario, it involves protecting all types of information transmitted through computer networks and categorizing them into different levels of encryption to meet various security requirements.

The second method is to encrypt files and substantive data in computer networks, including encryption of archives and databases.However, the encryption of stored information is relatively complex, as it faces the challenge of balancing computer data encryption and related information retrieval. Therefore, further research and development are needed for this encryption technology.

5.2 Ensure the integrity of information

To ensure that personal information is not maliciously altered, corresponding users can use cryptographic methods to generate matching results, namely network verification codes, by calculating network information and network data.When computer network users obtain network information, they should perform the same actual operation to obtain a new verification code, and then compare it with the received information verification code to confirm its consistency, in order to determine the accuracy of the network information.The cryptographic technique of using this type of information authentication can quickly detect whether user information is damaged.

5.3 Application of Digital Signature and Authentication Technology

In computer networks, the implementation of digital signature technology is achieved through the process of users signing electronic information.This method can be used for public key and private key encryption systems, but because it better meets practical applications and research needs, public key encryption systems are more commonly used.The use of digital signatures in computer networks mainly includes the following strategies: digital signatures on elliptic curves, digital signatures under finite automata, and so on. In addition, this also involves issues of national and regional laws and regulations. Many countries have established dedicated regulations to manage and guide the development of digital signature technology.

6. CONCLUSION

Today, due to the high popularity and wide application of the Internet, cryptography has become the core tool to protect network data security.However, relying solely on cryptographic methods cannot fully ensure the absolute security of network information, so it is necessary to comprehensively use multiple technologies to comprehensively improve the level of network security.Anyway, cryptography has always played a crucial role in the development of networks, and its continuous optimization has also provided more effective security for network information.

REFERENCES

[1] Diao, Su, et al. "Optimizing Bi-LSTM networks for improved lung cancer detection accuracy." PloS one 20.2 (2025): e0316136.

[2] X. Li, L. Evans, and X. Zhang, “Interactive data exploration for smart city analytics: A user-centered perspective,” 01 2025.

[3] Wang, J. (2025). Smart City Logistics: Leveraging AI for Last-Mile Delivery Efficiency.

[4] Bohang, Li, et al. "Image steganalysis using active learning and hyperparameter optimization." Scientific Reports 15.1 (2025): 7340.

[5] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.

[6] Yang, W., Zhang, B., & Wang, J. (2025). Research on AI Economic Cycle Prediction Method Based on Big Data.

[7] Xu, Haoran. "Sustainability Enhancement in Healthcare Facility Design: Structural and Functional Optimization Based on GCN." (2025).

[8] Jiang, Gaozhe, et al. "Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance." (2025).

[9] Tu, T. (2025). Log2Learn: Intelligent Log Analysis for Real-Time Network Optimization.