Journal of Artificial Intelligence Practice (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2024.070301
ISSN 2371-8412 Vol. 7 Num. 3

Application and Performance Evaluation of DES Data Encryption Algorithm in Computer Information Security Technology

Ying Ding[*]

IT Solution Consulting, MOYI Inc, New York, NY, USA
[*]*Corresponding author*

Keywords: Information technology, Confidentiality, encryption algorithms, DES algorithms, Information confidentiality technology, Performance evaluation, Information security

Abstract: This article delves into the application and performance evaluation of the Data Encryption Standard (DES) algorithm in computer information security technology. With the rapid development of information technology, information security issues are becoming increasingly prominent, especially in terms of confidentiality in data transmission and storage. In response to the inefficiency and increasingly complex security threats of traditional firewall technology, this article proposes a suggestion to use the DES algorithm as a more effective means of confidentiality. By evaluating and analyzing the performance of the DES algorithm in practical applications, the experimental results show that the DES algorithm performs well in maintaining encryption speed and decryption efficiency, but there are also some potential security vulnerabilities. This article aims to explore the application prospects of DES algorithm in the field of information security in depth, and propose improvement strategies to compensate for its security deficiencies. Our research will provide important references and insights for further development in the field of information security, helping to enhance the security and confidentiality of computer systems.

1. Introduction

With the development of technology, computer information encryption technology is constantly advancing. This article briefly introduces computer information encryption technology and explores its application in network security, providing reference for research in China.[1] In the field of computer security technology, data encryption algorithms are one of the important means to ensure information security. DES, as a classic symmetric encryption algorithm, has been widely used in this field. However, with the advancement of technology and attack methods, DES algorithms also face security challenges such as key length and cryptographic attacks. This article aims to explore the application and performance evaluation of DES in computer security technology, analyze its advantages, limitations, and challenges, and explore improvement directions to enhance the security and efficiency of security technology.

2. Related Research

In order to improve the ability to mine the demand for crude oil trade procurement prices and maximize the retention of valuable information, this paper proposes a crude oil trade procurement model based on the DEA Malmquist algorithm. The internal network should share the same database, with management personnel having independent access rights, while all registered users can exchange data between internal and external networks through QR code scanning; The sharing of internal and external network resources also enables suppliers and other registered users to immediately understand the procurement trends of the enterprise. Using DEA Malmquist algorithm combined with fuzzy theory, the uncertainty of procurement management was analyzed, and a refined procurement decision model with fuzzy parameters was established. The optimal ordering time and purchase quantity were determined using the symbol distance method and the center of gravity method. The experimental results show that this method can effectively retain valuable information in the initial sequence and has high practical application value for intelligent mining of material procurement needs. The proposed model achieved the highest accuracy of 98.62%.[1]

AbstrcatData encryption is the most basic technology of safety.DES algorithm and RSA algorithm are excellent.But they are still shortable in some other ways,such as process efficient,the key management etc.This paper analyzes the merit and the demerit of DES algorithm and RSA algorithm,and puts forward a new data encryption based on DES algorithm and RSA algorithm.[4]

Although the rapid development of the internet has greatly improved people's living and working conditions, providing convenient channels for information exchange, the data security of network transmission is increasingly being concerned, especially for critical accounting data. Once these data are obtained and utilized by hackers, it may cause serious damage to the data owner. Based on this background, this article aims to study the encryption of accounting data using DES algorithm in computing environments. We propose an improved quantum genetic algorithm and apply it to the S-box design of DES algorithm to enhance the nonlinear characteristics of the S-box, reduce the risk of differential analysis, and improve the security of DES algorithm.[7]

With the popularization of information technology, computer networks have become an indispensable part of people's lives, providing convenience for communication and exchange. As a result, network security issues are becoming increasingly prominent, especially in the area of enterprise data transmission and storage. To ensure the security and integrity of data, enterprises need to adopt effective information security protection strategies. A comprehensive information security assessment method considering the network environment is proposed to address the current challenges faced by information security, in order to guide the implementation of enterprise information security protection work and provide a certain reference for evaluating the effectiveness of protection measures.[8]

3. Application and Performance Evaluation of DES Data Encryption Algorithm in Computer Information Security Technology

3.1 Overview of DES algorithm

DES (Data Encryption Standard) is a symmetric cryptographic algorithm that uses keys of the same length for encryption and decryption. Its key length is 64 bits, including 8 bits of parity, so the effective key length is 56 bits. During the DES encryption process, plaintext undergoes 16 rounds of encryption transformation. The following figure (figure 1) shows its calculation process:

Firstly, the plaintext undergoes initial permutation to obtain the left and right parts, followed by the key generation process to generate a 48 bit sub key. Next, through 16 rounds of encryption transformation, each transformation includes operations on the left and right parts and the application of sub keys. Finally, after inverse initial permutation, the final 64 bit ciphertext is obtained. The DES algorithm ensures the secure transmission of data through complex encryption processes and key generation mechanisms. A system for encryption, including a Message Management Module (MMM); Restricted Secret Server (RSS), including a Restricted Secret Server Network Interface (RSS-NI) connected to the MMM and including at least one Very Large Key (VLK) module.

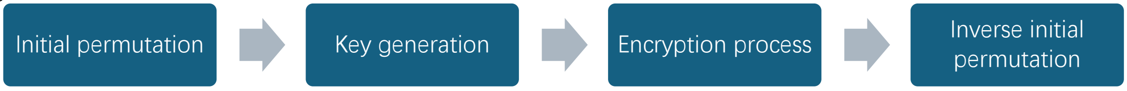

Figure 1: The calculation process of DES data encryption algorithm

The history of DES algorithm can be traced back to the early 1970s, when the National Bureau of Standards (NBS, now NIST) of the United States released DES as the standard for data encryption. DES has undergone rigorous evaluation and review, becoming the first widely adopted encryption standard. With the improvement of computer performance and the development of cryptography, DES has gradually exposed its security vulnerabilities. Its key length is relatively short and it is susceptible to brute force attacks. However, in the following years, the use of DES gradually decreased and was replaced by more secure encryption algorithms.

Although the security of DES is highly controversial, it plays an important role in the development of cryptography and computer security. The design concept and structure of DES provide valuable experience and inspiration for subsequent encryption algorithms, especially in key management, permutation networks, and S-box design. The widespread application of DES has also promoted research in the fields of cryptography and information security, promoting the birth and development of a new generation of encryption algorithms.

3.2 The Application of DES Data Encryption Algorithm in Computer Information Security Technology

The DES algorithm has a wide range of applications in computer information security technology, mainly reflected in the following aspects:

Data transmission encryption is a common measure in the field of network security, among which DES algorithm is usually used to ensure the security of data during network transmission. By encrypting data, it is possible to effectively prevent unauthorized visitors from stealing or tampering with the data, thereby ensuring the confidentiality and integrity of data transmission. For example, this system adopts an improved data encryption algorithm (DEA) and builds a hardware system with the help of CPLD chips. In the process of data transmission, the sound wave signal is sent to the receiving end after frequency modulation and key encryption. After filtering and key decryption at the receiving end, the original signal can be restored, thus achieving encrypted transmission within the closed-loop range. The experimental results of Reinhold indicate that the system has high security and is suitable for the transmission of confidential or sensitive signals.[2]

Data storage encryption is an important measure to protect data stored in computers or servers. DES uses encryption technology to convert data. Even if the data is illegally obtained, the content cannot be interpreted, but it effectively maintains the privacy of users and the confidentiality of sensitive information. For example, companies can use DES algorithms to encrypt and store personal and financial data of employees to reduce the risk of internal and external data leakage and ensure information security. Encryption protocol is a crucial security mechanism in network communication and data transmission. The DES algorithm, as one of the classic encryption techniques, plays an important role in the implementation of protocols such as SSL/TLS and IPsec. These protocols use DES algorithms to encrypt and decrypt data to ensure the confidentiality and integrity of communication. For example, the SSL/TLS protocol uses the DES algorithm to encrypt communication data between websites and browsers, in order to resist threats such as man in the middle attacks and data theft.

The application and performance evaluation of DES data encryption algorithm in computer information security technology need to comprehensively consider its advantages and disadvantages. Although DES has been widely used and played a crucial role, its limitations have gradually become apparent with the advancement of technology and the improvement of safety requirements. The DES algorithm has a relatively short key length, making it vulnerable to password attacks such as brute force cracking. Although DES has undergone rigorous evaluation and review in its design, the continuous progress of modern cryptographic attack methods has weakened its security. In the current information security environment, we need to comprehensively evaluate the applicability of DES algorithms and consider adopting other more secure and efficient encryption algorithms to ensure the security and integrity of data. As is well known, both DES algorithm and RSA algorithm are excellent, but there are still shortcomings in processing efficiency, key management, and other aspects.[3]

3.3 Performance evaluation of DES algorithm

Encryption speed evaluation: Although DES algorithm can achieve high encryption speed in hardware implementation, it may be limited in software implementation. In practical applications, it is necessary to evaluate the encryption speed based on specific application scenarios and system environments to ensure that it can meet practical needs. The following (Table 1) compares the encryption speeds of DES algorithm and AES algorithm under different data volumes [5].

Table 1: Comparison chart of encryption speed between DES algorithm and AES algorithm under different data volumes

Data volume(MB)	DES encryption speed(Mbps)	AES encryption speed(Mbps)
1	10	50
10	5	40
100	2	30
1000	1	20

Security assessment: Although the DES algorithm is no longer secure in modern cryptographic environments, it can still be used in certain specific low security requirements scenarios. For example, combining data mining techniques to analyze and process data in computer networks has optimized information security protection work.[4] In practical applications, some enhancement measures can be taken to improve the security of DES algorithms, such as increasing key length and using more complex key generation algorithms.

Scalability: The scalability of DES data encryption algorithms is limited by their design. Firstly, the DES algorithm uses a fixed key length of 56 bits, which is considered relatively short in modern cryptographic environments and may not provide sufficient security guarantees. Secondly, the design of DES algorithm is relatively simple, and with the improvement of computing power and the development of cryptographic attack technology, its ability to resist modern attack techniques is relatively weak. The encryption and decryption process is relatively time-consuming, especially when dealing with large-scale data, which may lead to performance bottlenecks. Moreover, due to the fixed and short key length of the DES algorithm, key management and distribution may become complex, especially in large-scale systems.

3.4 Improvement and optimization of DES algorithm

Computer network technology is crucial in electronic information engineering, enriching functions, improving efficiency and quality. However, in the face of complex information environments, we need to pay more attention to network system security to ensure quality of life. Improving and optimizing DES algorithms is a key research area aimed at enhancing their security and performance. In response to the shortcomings of the standard implementation of DES algorithm, the implementation of DES algorithm has been proposed and improved, which can encrypt (or decrypt) random long strings or files.[3]For example, the system adopts an improved data encryption algorithm (DEA) and uses the CPLD chip EPM570 to build a hardware encryption system. After frequency modulation, the acoustic signal is encrypted by a key and transmitted to the receiving end. After decryption, the original signal is restored, achieving close range encrypted transmission. The hardware circuit of the transmitter and receiver includes the main controller, CPLD, DDS, filter, and RS module circuit.[7]In addition, alternative algorithms such as Advanced Encryption Standard (AES) have also been widely studied and applied. The AES algorithm adopts a longer key length and exhibits higher speed and security during encryption and decryption processes. On the other hand, technologies such as hardware acceleration support, parallel processing optimization, and key management improvement have also received attention from researchers [6].

4. Results and Discussion

Conduct in-depth research and evaluation on the application and performance of DES data encryption algorithm in computer information security technology. After investigation and analysis of practical application scenarios and performance, the following conclusion can be drawn: DES algorithm is widely used in some low security scenarios, such as traditional legacy systems and storage schemes that do not require high data sensitivity. However, in environments that require higher security, DES algorithm is gradually being replaced by more secure and efficient encryption algorithms, such as AES algorithm.

In terms of performance evaluation, it was observed that the DES algorithm has a relatively slow encryption speed in software implementation, especially when dealing with large-scale data, and performs poorly. In terms of security evaluation, DES algorithm is limited by key length and algorithm design, which makes its ability to resist cryptographic analysis attacks relatively weak. The DES algorithm adopts fixed length keys and a simple algorithm design, which has certain limitations in large-scale data processing and high security requirements, and its scalability is limited.

Overall, although the DES algorithm still has practical value in certain situations, its security and performance can no longer meet the requirements of modern information security. Therefore, future research directions should include exploring more secure encryption algorithms, improving the performance and security of DES algorithms, and researching encryption schemes suitable for large-scale data processing. Through continuous research and innovation, the level of computer information confidentiality technology can be further improved to better respond to the growing security threats and challenges.

5. Conclusion

With the improvement of technological level in our country, computer networks have become an indispensable part of daily life, promoting social and economic development. Under the new information security requirements, we need to attach importance to relevant work and take effective measures and strategies, such as firewall technology, encryption technology, network access control technology, and network virus prevention technology.Although DES in this article is still widely used in some low security scenarios, its performance and security limitations in the face of high security requirements and large-scale data processing pose challenges. Especially in terms of encryption speed, security, and scalability, there are limitations. Therefore, future research should focus on improving the performance and security of DES algorithms, or finding encryption solutions that are more suitable for modern information security needs.

References

[1] Yan L. Research on Crude Oil Trade Procurement Model Based on DEA-Malmquist Algorithm [J]. Scientific programming, 2021, (14): 20-21.

[2] Reinhold A G. System And Method For Securely Encrypting Data: US17125887 [P]. US20210152532A1 [2024-04-14].

[3] Shan Huilin, Zhang Yinsheng. Sound wave encrypted transmission system based on improved DEA algorithm [J]. Electronic technology application, 2019, (4): 5. DOI: CNKI: SUN: DZJY.0.2019-04-024.

[4] Hao W U. Data encryption means based on DES Algorithm and RSA Algorithm [J]. Journal of Jiaozuo Institute of Technology, 2002.

[5] Wu H, Wu H. Research on Computer Network Information Security Problems and Prevention Based on Wireless Sensor Network[C]. Asia-Pacific Conference on Image Processing, Electronics and Computers. 2021. DOI:10.1109/ IPEC51340.2021.9421303.

[6] Huilin S, Yinsheng Z. The acoustic encryption transmission system based on improved DEA [J]. Application of Electronic Technique, 2019.

[7] Wu Y, Dai X. Encryption of accounting data using DES algorithm in computing environment [J]. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 2020, (1): 39.

[8] Guo Y, Xu J, Yuan H, et al. Research on Enterprise Computer Network Security Protection Technology Based on Information Technology[C]. International Conference on Automation, Electronics and Electrical Engineering. 2020. DOI:10.1109/AUTEEE50969.2020.9315704.