Optimization of Data Encryption Technology in Computer Network Communication

Jun Lin [1,*], Zhiqi Shen [2]

[1] *The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore, Singapore*

[2] *School of Computer Science and Engineering, Nanyang Technological University, Singapore, Singapore*

(Received: September 17, 2023; Revised: October 12, 2023; Accepted: November 20, 2023; Available online: December 10, 2023)

Abstract

In recent years, the pervasive integration of computer network communication systems across various industrial domains has revolutionized daily life and work, offering unprecedented convenience. Recognizing the paramount importance of securing these communication channels, this paper meticulously examines the current landscape and distinctive features of data encryption technology in computer network communication security. To comprehend the evolving threat landscape, the paper elucidates prevalent security challenges confronting contemporary networks. Subsequently, the study delves into a comprehensive discussion on the implementation of data encryption technology to fortify network communication security. This includes a nuanced exploration of link encryption technology, node encryption technology, and end-to-end encryption technology, elucidating their respective roles and effectiveness. Moreover, the paper undertakes a profound analysis of the practical application of data encryption technology within the realm of computer network communication security. Employing empirical evidence, the study reveals significant findings, such as the Mean Squared Error (MSE) values for data sets. Specifically, the MSE value for data 1 is recorded at 42.453, data 2 at 87.324, and data 3 at 87.324674. These findings provide invaluable insights into the performance and efficacy of data encryption technology in safeguarding computer network communications, paving the way for enhanced security measures in the dynamic and ever-expanding digital landscape.

Keywords: Computer, Network Communication, Data Encryption

1. Introduction

With the rapid development of China's economy, the level of scientific and technological intelligence and information intelligence is deepening. This is the only way of scientific development, but the development of society has gradually put forward higher requirements and challenges for computer network information technology. In the era of big data, computer and Internet technology bring more convenience to people's life and work, but also leave a lot of security risks. We must solve the problems of information security and data theft when people use computers.

With the continuous progress of science and technology, many people have studied data encryption technology. For example, some domestic teams have studied the field of computer network communication.Compared with bio IBE scheme, this scheme reduces the cost. Based on the idea of Abe, this paper proposes a ciphertext policy hidden vector encryption (cphve) scheme which supports multi-user encryption and search operation at the same time. The scheme uses attribute based access policy to encrypt keywords. When the user's attributes conform to the policy, they can search for keywords. This paper proposes a protocol to distribute session key effectively in this environment to establish a secure channel. Suppose that the target network consists of many local trusted centers, and each center has many users connected to it. This scheme combines the concept of public key distribution and RSA encryption scheme as a

*** Corresponding author: Jun Lin (junlinlin@ntu.edu.sg)**
DOI: https:// doi.org/10.47738/ijaim.v3i4.65

basic mathematical tool, but eliminates the related storage problems [1]. Some experts have studied the network transmission encryption algorithm of vector data, and proposed a new hybrid encryption technology, which can use the payload field of multi connection streams as the carrier. This technology is mainly divided into three stages. Firstly, the state of the network is analyzed. Then, the insertion point is selected according to the protocol, the hidden data is inserted into the packets injected into the network. In this paper, we evaluate the hybrid covert method and user datagram protocol (UDP) connection under two kinds of network load, and make a trade-off analysis between throughput and detectability. This paper discusses the important security features that make the wireless network more stable. It includes the important module of building WLAN security, secure data transmission, data encryption, wireless security type and other issues, making it a more stable platform to provide and build secure digital network. In this paper, we propose a method to ensure security as long as at least one party is trustworthy and the other party may be corrupt. Before the detailed OPNET simulation to evaluate the cost of the new method compared with the standard GSM, the pseudo collision probability is derived through analysis [2]. Some experts have studied data encryption and key management, and summarized the implementation of a secure data authentication model for wireless body area network, which uses a single private key to exchange in the configuration process. A secure WBAN system is proposed, but the security parameters need to be added in WBAN system. Existing systems must ensure the security of using limited resources. Trying to solve these security problems, considering the limitation of available power, bandwidth and other resources, helps to achieve a more secure and time-saving system in place, and provides an effective online health monitoring scheme for WBAN [3]. Although the research results of data encryption technology are quite abundant, there are still some shortcomings in the data encryption technology of computer network communication.

In order to study the optimization of data encryption technology in computer network communication, this paper finds the long-term and short-term storage network through the research of computer network communication and data encryption technology. The results show that this method is conducive to the optimization of data encryption technology in computer network communication.

2. Literature Review

2.1. Information Security in the Era of Big Data

The swift evolution of China's economy has catapulted the nation into an era where scientific and technological intelligence, coupled with information intelligence, serves as the linchpin for progress. This paradigm shift, however, is not without its challenges. The escalating reliance on computer network information technology, particularly in the ubiquitous era of big data, has ushered in a multitude of conveniences for individuals and organizations alike. This convenience, however, comes at a price – an increased susceptibility to information security breaches and data theft during computer usage.

The burgeoning complexities of the contemporary technological landscape necessitate a comprehensive understanding of the threats posed to information security. Research in this domain aims not only to identify these threats but also to devise innovative solutions that can safeguard sensitive information. Numerous scholars have delved into the intricacies of information security, highlighting the importance of robust encryption technologies to mitigate the risks associated with the digital age [13].

2.2. Advancements in Data Encryption Technology

In response to the intensifying need for heightened information security, a significant body of research has been devoted to the exploration of data encryption technologies. One noteworthy example is the ciphertext policy hidden vector encryption (cphve) scheme, which has garnered attention for its ability to support multi-user encryption and simultaneous search operations. This scheme, anchored in attribute-based access policies, not only demonstrates a nuanced understanding of security challenges but also endeavors to reduce costs when compared to alternative encryption methodologies, such as the bio Identity-Based Encryption (IBE) scheme [14].

As technology continues to advance, researchers are actively engaged in refining encryption techniques to address emerging threats. The dynamic nature of cyber threats necessitates an adaptive approach to encryption, prompting

scholars to explore innovative cryptographic solutions that align with the evolving landscape of computer network communication [14].

2.3. Network Transmission Encryption and Hybrid Technologies

The intricate dance between security and efficiency in network transmission encryption algorithms has been a focal point of investigation. Researchers have probed the challenges posed by vector data and put forth innovative solutions to enhance the security of data during transmission. Hybrid encryption technologies, a noteworthy advancement in this domain, leverage the payload field of multi-connection streams as carriers for hidden data. The deployment of these technologies involves meticulous stages, encompassing network state analysis, insertion point selection, and the discreet embedding of hidden data into network packets. Evaluation studies have been conducted to dissect the delicate balance between throughput and detectability under varying network loads and protocols, contributing to a more nuanced understanding of the trade-offs inherent in encryption methodologies [15][16].

2.4. Wireless Network Security and Optimization

The paradigm of wireless network security has witnessed remarkable strides in research endeavors, seeking to fortify the foundations of secure digital networks. Exploring crucial components such as WLAN security modules, secure data transmission, data encryption, and wireless security types, scholars aim to establish a robust framework that not only mitigates existing vulnerabilities but also anticipates and addresses emerging threats. The synthesis of public key distribution, RSA encryption schemes, and the elimination of storage-related issues showcases the innovative approaches taken to bolster the security infrastructure of wireless networks [17][18].

Moreover, the recognition that security is contingent on trustworthiness introduces novel paradigms where secure communication is possible even in scenarios where one party may be susceptible to corruption. This conceptual shift marks a significant contribution to the discourse on wireless network security, opening avenues for further exploration [17][18].

2.5. Secure Data Authentication in Wireless Body Area Networks (WBANs)

The unique challenges posed by wireless body area networks (WBANs) have spurred dedicated research efforts in the realm of data encryption and key management. Scholars have synthesized secure data authentication models for WBANs, utilizing a single private key exchange during the configuration process. While these efforts have yielded significant strides in establishing secure WBAN systems, there is a recognized need to augment security parameters within the system architecture. This recognition is driven by the imperative to ensure security in the face of limited resources, including power, bandwidth, and other constraints inherent in WBANs [19][20].

As researchers continue to navigate the delicate balance between security and resource efficiency in the context of WBANs, the need for a secure and time-saving online health monitoring scheme remains paramount. This underscores the ongoing quest for solutions that not only fortify security measures but also optimize the utilization of limited resources for more effective and resilient WBANs [19][20].

3. Methodology

3.1. Computer Network Communication

The computer security network communication management module is an intermediate module connecting the trusted guarantee server and the trusted cloud computing server[4]. It is used to establish a reliable connection between cloud computing server and trusted Assurance server[5]. The trusted cloud computing server requests to join the cloud environment, and the communication operations such as establishing and disconnecting the connection for the trusted function request need to be realized through the security communication management module[6]. Similarly, all connected trusted cloud computing servers in the cloud environment are managed by the security communication management module, and all requests to the trusted security server are processed and responded by the module[7].

3.2. Data Encryption Technology

3.2.1. Data encryption technology

Of course, there are many algorithms, and there is no final conclusion[8], and there is no strict standard implementation[9]. The algorithm has been developing continuously and is always optimized[10]. As long as it is convenient to use in a certain time and certain environment, it can be used. Encryption algorithm is a process of generating unreadable ciphertext through a series of operations and transformations between the original plaintext and the key. The key and algorithm are of great significance to the encryption process. The key is also an algorithm. It is formed by a specific algorithm. It is usually encapsulated in a class library in a program and can be called directly.

3.2.2. Symmetric encryption algorithm

Controller layer encryption technology, also known as physical layer encryption technology, refers to the encryption and decryption algorithm and key added to the controller, through hardware to achieve data encryption and decryption, encryption speed and key management costs are very small, file system layer encryption is the same, is a transparent encryption and decryption technology. But the controller layer encryption uses the same key to encrypt all the data stored in the FLA device. This is a comprehensive encryption method, encryption particles are too large[11].

3.2.3. The importance of data encryption

The best of data security is to prevent data leakage through file encryption. Before transmission, the data is encrypted, converted into ciphertext, and then transmitted. Even if it is intercepted or copied in the process of transmission, the data can not get the correct information. Encryption method: encryption data. However, the encrypted data is easy to lose its availability and business attributes, which is difficult to develop and use. This method is only suitable for business scenarios with strong demand for data protection, such as irreversible algorithms for group information statistical analysis, such as data table mapping, algorithm mapping, etc., such as irreversible algorithms for random interference and scene disorder, reversible algorithms for location conversion, etc., which can ensure the reversibility of business attributes. As encryption technology is the most basic and core technical means of network information, the effectiveness of encryption depends on the encryption algorithm. Through the physical protection and encapsulation of encryption card, the whole encryption process is transparent, which makes the security foundation of the whole system stable and firm. The hardware platform chooses the trusted platform recognized by the industry, namely industrial control computer, which effectively ensures the security of the hardware foundation of the system. The whole process of encryption and key management is encapsulated on the security card whole system[12].

3.3. Long Term and Short Term Memory Network

The network structure of long-term and short-term memory fuses long-term and short-term memory by adding gate control, which solves the problem that only short-term memory is generated due to RNN gradient disappearance to a certain extent, as shown in equation (1):

$$f_t = \sigma(W_f[h_{t-1}, x_t + b_f) \tag{1}$$

Accuracy B is the ratio of the total number of correct text detection boxes to the total number of all text detection boxes; recall rate is the ratio of the total number of correct text detection boxes to the total number of real labeled text detection boxes; C measure can comprehensively evaluate accuracy B and recall rate. Where h is the real annotation text detection box, W is the text detection box to be predicted, which represents the best match real annotation text detection box, and represents the best match actual text detection box, as shown in formula (2):

$$C_t = tan(W_c[h_{t-1}, x_t + b_c]) \tag{2}$$

As the key element of encryption, the larger the key space is, the more times the algorithm is exhausted, and the more difficult it is to crack. Therefore, the size and complexity of key space are closely related to the security of vector geographic data encryption algorithm. If the length of the key is set to R, the size of the key space * (3) is calculated as follows:

$$P_{rec} = \frac{N_{rec}}{N_{total}} \tag{3}$$

The m after operation is related to the size of N. the larger the total number of data n is, the larger the range of key value is. The key space of integer key is (4):

 ISSN 2776-8007

$$K_m = N \tag{4}$$

4. Experience

4.1. Extraction of Experimental Objects

In order to improve the security of scrambling,group the sequence if the whole sequence is cracked. Different groups have different scrambling keys. The length of packets is closely related to the efficiency of scrambling.different packet length on the efficiency of scrambling algorithm, experiments are carried out on the sequences with N length, and the sequences are divided into 1-N groups. After grouping, each group is simply scrambled in the group, and the time required for the operation of the whole sequence under different packet lengths is analyzed. No matter how long the package is, the length of the sequence generated by the 3D sequence is the total length of the data. Therefore, the generation and processing time of scrambling key are not included in the calculation of sequence encryption efficiency.

4.2. Experimental Analysis

After the network equipment receives the message, the processing flow is: first, restore the message content to the format according to the code, then analyze the message, analyze the syntax correctness, and verify the version and authentication information. If the syntax is correct and the validation is passed, the valid data will be further separated and displayed to the administrator. If necessary, according to the data corresponding operation, and return the reply information. After the failure of parsing or verifying the validity of the packet, the parsing module returns the captured packet, reports the exception to the management side, and discards the received message. A unique integer set by a network device for each packet, by which different instructions can be distinguished. Because in fact, the request is handled by the underlying program. When the response packet arrives, the program should compare the request number in the packet with that in the previous packet. The request number is also used to identify duplicate messages. In order to make up for the defects of the protocol and ensure the security of the network management system, a new security mechanism is introduced. Asymmetric encryption algorithm, because of its good security characteristics, can solve the problems of packet information being easily stolen, tampered and simple authentication mechanism, and become a better choice to make up for security defects.

5. Discussion

5.1. Encryption Effect

In order to quantify the security of encryption, the point set before and after encryption can be used to evaluate the security of encryption. MSE is a measure of the difference between the two. The MSE, encryption effect, as shown in Table 1.

Table 1. Encryption security experiment

data	MSE
Data 1	42.453
Data 2	87.324
Data 3	124.674

It can be seen from the above that the MSE value of data 1 is 42.453, the MSE value of data 2 is 87.324, and the MSE value of data 3 is 124.674. The results are shown in Figure 1.

 ISSN 2776-8007

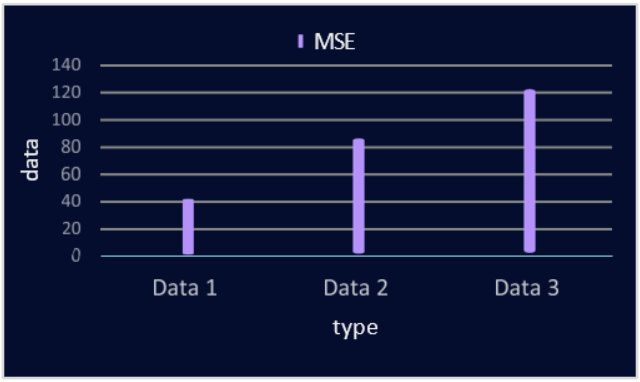

Figure 1. Encryption security experiment

Through the MSE value of the data before and after encryption, we can see that the data before and after encryption has a great degree of difference, the interference to the data is great, the encryption effect is very good, and the availability of the data is damaged.

5.2. Encryption Efficiency

On the premise of ensuring security, the pursuit of algorithm efficiency is a problem that can not be ignored. In order to verify the effectiveness of the algorithm, the above four kinds of data are encrypted and decrypted respectively. At the same time, in order to compare the efficiency of the algorithm with the classical symmetric classical simulated in MATLAB, and the above data is encrypted and decrypted with AES algorithm, as shown in Table 2.

Table 2. Data encryption algorithm based on step-by-step encryption

Data	Point	Size	Encryption time (s)
Data A	532.34	36KB	1.42
Data B	656.43	38KB	5.92
Data C	678.42	74KB	2.84
Data D	721.43	94KB	3.73

As can be seen from the above, the number of data a is 532.34, the size is 36KB, and the encryption time is 1.42s; the number of data B is 656.43, the size is 38KB, and the encryption time is 5.92s; the number of data C is 678.42, the size is 74KB, and the encryption time is 2.84s; the number of data D is 721.43, the size is 94kb, and the encryption time is 3.73s. The results are shown in Figure 2.

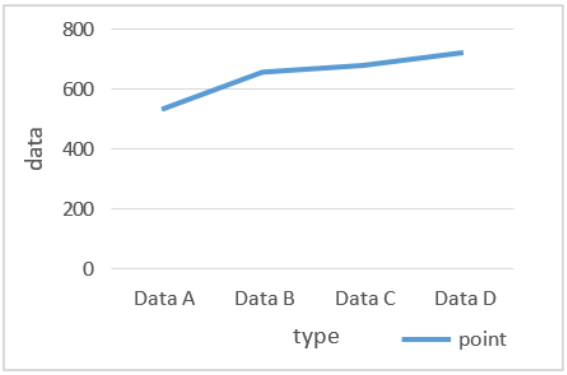

Figure 2. Data encryption algorithm based on step-by-step encryption

It can be seen from the above that with the increase of the number of points, the time required for data encryption and decryption is correspondingly longer, but the overall efficiency requirements are met.

6. Conclusion

In recent years, information communication technology and Internet technology have developed rapidly. The computer network communication system has been widely used in various fields, which brings great convenience to people's daily life and study. A series of security issues are more and more concerned by people. This paper describes the application of data encryption technology in the security of computer network communication. Combined with the current application situation, the paper discusses its existing application technology and analyzes a new application technology with higher performance. This paper introduces the data encryption technology of computer network communication and the application of data encryption technology in network communication, aiming to provide some ways healthy and orderly network communication.

7. Declarations

7.1. Author Contributions

Conceptualization: J.L. and Z.S.; Methodology: Z.S.; Software: J.L.; Validation: J.L. and Z.S.; Formal Analysis: J.L. and Z.S.; Investigation: J.L.; Resources: Z.S.; Data Curation: Z.S.; Writing Original Draft Preparation: J.L. and J.L.; Writing Review and Editing: Z.S. and J.L.; Visualization: J.L.; All authors have read and agreed to the published version of the manuscript.

7.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.4. Institutional Review Board Statement

Not applicable.

7.5. Informed Consent Statement

Not applicable.

7.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

References

[1] Gong Lina, et al., "The Application of Data Encryption Technology in Computer Network Communication Security," *AIP Conference Proceedings*, vol. 1834, no. 1, pp. 1-5, 2017.

[2] Fan A, Wang Q, Debnath J, "A high precision data encryption algorithm in wireless network mobile communication," *Discrete & Continuous Dynamical Systems*, vol. 12, no. 4&5, pp. 1327-1340, 2019.

[3] Kiarie L K, Langat P K, Muriithi C M, "Application of Spritz Encryption in Smart Meters to Protect Consumer Data," *Journal of Computer Networks and Communications*, vol. 2019, no. 3, pp. 1-10, 2019.

[4] Vidal José R, Pla Vicent, Guijarro Luis, "Flexible Dynamic Spectrum Allocation in Cognitive Radio Networks Based on Game-Theoretical Mechanism Design," *Lecture Notes in Computer Science*, vol. 6641, no. 11, pp. 164-177, 2017.

[5] Li Xirong, "Tag Relevance Fusion for Social Image Retrieval," *Multimedia Systems*, vol. 23, no. 1, pp. 29-40, 2017.

[6] Groza B, Murvay S, Herrewege A V, et al., "LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 3, pp. 1-28, 2017.

[7] Vyas B, Vajpayee A, "Local Data Security Through Encryption," *International Journal of Emerging Trends & Technology in Computer Science*, vol. 47, no. 2, pp. 137-141, 2017.

[8] Tang X, Tan L, Hussain A, et al., "Three-dimensional Voronoi Diagram-based Self-deployment Algorithm in IoT Sensor Networks," *Annales des Télécommunications*, vol. 74, no. 7-8, pp. 517-529, 2019.

[9] Kumar S, Yadav S, Kumar D, "Secured Communication using Data Dictionary through Triple DES," *International Journal of Computer Applications*, vol. 166, no. 3, pp. 40-44, 2017.

[10] Khalil M I, "Medical Image Steganography: Study of Medical Image Quality Degradation when Embedding Data in the Frequency Domain," *International Journal of Computer Network and Information Security*, vol. 9, no. 2, pp. 22-28, 2017.

[11] Bernardini C, Marchal S, Asghar M R, et al., "PrivICN: Privacy-preserving content retrieval in information-centric networking," *Computer Networks*, vol. 149, no. 1, pp. 13-28, Feb. 11, 2019.

[12] M. Klügel et al., "Joint Cross-Layer Optimization in Real-Time Networked Control Systems," in *IEEE Transactions on Control of Network Systems*, vol. 7, no. 4, pp. 1903-1915, Dec. 2020, doi: 10.1109/TCNS.2020.3011847.

[13] Z. Bian, "Analysis of Computer Network Information Security in the era of Big Data," *Advances in Intelligent Systems and Computing*, vol. 1, no. 1, pp. 1054–1059, 2020. doi:10.1007/978-981-15-2568-1_145

[14] L. Li, "Application of data encryption technology in Computer Network Information Security," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1–8, 2022. doi:10.1155/2022/7472205

[15] G. Lisanawati and J. E. Kehinde, "When Technology Meets Money Laundering, What Should Law Do? New Products and Payment Systems and Cross Border Courier," *Int. J. Informatics Inf. Syst.*, vol. 5, no. 3, pp. 142–149, Sep. 2022

[16] X. Gao, J. Mou, S. Banerjee and Y. Zhang, "Color-Gray Multi-Image Hybrid Compression–Encryption Scheme Based on BP Neural Network and Knight Tour," in *IEEE Transactions on Cybernetics*, vol. 53, no. 8, pp. 5037-5047, Aug. 2023, doi: 10.1109/TCYB.2023.3267785.

[17] S. N. Maharani, B. Sugeng, M. Makaryanawati, and M. M. Ali, "Bank Soundness Level Prediction: ANFIS vs Deep Learning," *J. Appl. Data Sci.*, vol. 4, no. 3, pp. 175–189, Sep. 2023,

[18] M. M. Hasan and H. T. Mouftah, "Optimization of Watchdog Selection in Wireless Sensor Networks," in *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 94-97, Feb. 2017, doi: 10.1109/LWC.2016.2633990.

[19] A. P. Wibawa et al., "Mean-Median Smoothing Backpropagation Neural Network to Forecast Unique Visitors Time Series of Electronic Journal," *J. Appl. Data Sci.*, vol. 4, no. 3, pp. 163–174, Aug. 2023

[20] S. Jegadeesan, M. Azees, N. Ramesh Babu, U. Subramaniam and J. D. Almakhles, "EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs)," *in IEEE Access*, vol. 8, no. 1, pp. 48576-48586, 2020, doi: 10.1109/ACCESS.2020.2977968.