Research on Security Technology of Network Communication Information Based on Double Encryption

Xiaolong Fan
Lanzhou Institute of Technology, Lanzhou, Gansu, China

Corresponding author’s e-mail address: 120839127@qq.com

Abstract. Data is transmitted from the server to the terminal or the terminal to the server during the transmission process, the data information is easily monitored or tampered with, which will cause information leakage or data display false data. If the wrong instruction information may be received in the industrial control field, it will bring a lot to industrial production. Hazards and losses, so in order to ensure the reliability and data security of the network communication between the terminal and the server, industrial equipment and management system, it is very necessary to use secure communication connections and reliable data encryption algorithms to ensure communication and data security. This paper proposes an improved AES and MD5 hybrid encryption scheme, which uses SSL to encrypt the transmission channel during the communication process, uses the improved symmetric encryption algorithm AES to encrypt the data in network transmission, and encrypts the data at the sending end. Then use the improved MD5 to generate a digital fingerprint for the encrypted data. At the receiving end, use MD5 to generate the same fingerprint for the encrypted data sent, and use the digest fingerprint verification to determine whether the data has been tampered with or lost during transmission. It is possible to greatly improve the security and reliability of system communication and data.

Keywords. Data encryption, communication security, digital fingerprint

1. Introduction
As informatization continues to penetrate into all walks of life, the economic form and social form based on Internet information have become an unstoppable world trend. In order to adapt to the rapid development of information technology, the intelligentization of industrial production and networking has become an inevitable trend of development. The open Internet information environment also contains defects that cannot be ignored. With the large-scale application of information and the Internet, network and data security become the biggest hidden danger. Especially in China, half of the data security caused by the Java vulnerabilities in 2013 was national government agencies and the financial industry. Although the data leaked by the financial industry is not confidential data of financial institutions, the existence of people's information leakage cannot be ruled out. In recent years, losses caused by personal information data leakage have reached tens of billions of dollars worldwide, so it is urgent to solve the security problem. Software is the soul of the information industry and equipment. Therefore, active information encryption and secure sockets have become an inevitable
choice for information security and the industry. A reasonable software security mechanism can effectively prevent the greatest possible data theft and tampering.

2. Research status at home and abroad
With the widespread penetration of smart portable devices, the competition for IoT devices has become increasingly fierce. The intelligent era is also about to enter the manufacturing sector. And form new challenges and development trends as well as new industry patterns and standards in the global manufacturing industry. Many governments and scientific research institutions in the world regard it as a national strategy, and have issued a variety of policies to ensure the reliability of the goal. For example, in recent years, the German government has vigorously promoted the high-tech strategy based on cyber-physical systems and the Internet of Things, hereinafter referred to as "Industry 4.0"[1], and my country's "Made in China 2025" manufacturing strategy, focusing on "smart factories" and "The two themes of "intelligent production" aim to promote the transformation of the manufacturing industry to the intelligent field[2].

The Chinese government has successively issued system policy documents in recent years, recommending the deep integration of manufacturing industrial control systems and information systems, which is intended to promote the adjustment of traditional manufacturing industrial control systems and the advancement of intelligent manufacturing [3]. The National Electronic Information Industry Development Fund project "Development and Application Demonstration of Distributed Numerical Control System (DNC) for Discrete Manufacturing" also included it as an important research object[4].

3. Analysis of Main Technologies of Network Communication Information Security
Network security is a research topic related to computer science and communication [5]. Specifically, the applicable scenarios of network security research include the technology, system and service of processing and transmitting information [6]. The system generally refers to the laws and regulations designated by local or national governments for information security to achieve the methods of protecting information security; Service generally refers to safe and reliable solutions provided by ISP providers; Technology is a concrete realization [7]. For us, laws and regulations and ISP services are unreliable parts, because the current laws and regulations have clearly stipulated the maximum punishment and determination rules for information security crimes, and ISPs have also provided the greatest possible reliability Web environment [8]. But even so, our information security is still torn, so we can only solve the problem from the technical level aside from the above two levels, and in the field of technology is limited by the applicable scenarios of hardware protection, so we can only choose software technology solutions.[9]

3.1. Secure Socket Layer Technology
The main technical solutions for network communication security are mainly reflected in connection encryption, connection isolation, and network stream data encryption. The scope of application includes but not limited to the following scenarios:

(1) Isolated network connection, such as bank network system.
(2) Hardware-based channel isolation (applicable to internal Internet, security attributes are provided by routers).
(3) Secure network transmission and sockets [34], such as TLS, SSL.
(4) Network stream data encryption, such as string encryption.

Among the above three items: (1) are limited by the impact of ISP and equipment physical environment, as well as R&D and operation costs(2) Limited by the limitations of hardware scenarios. Therefore, according to the application scenarios and technical requirements of the workshop management system and industrial production equipment, encryption uses items (3) and (4) respectively.
Secure network transmission includes but is not limited to SSL/TLS. The article uses SSL as a technical solution for transmission security. SSL is a de facto secure socket standard, located between various application layer protocols.

At present, the more commonly used SSL frameworks have their own implementation schemes in large technology companies to ensure data reliability [10]. However, for enterprises and institutions with insufficient capacity and budget, if they need to use secure sockets, they choose to use open source frameworks. There are many open source secure socket implementations, but the most famous one is Openssl [11]. Openssl has been embedded in the Linux system level. But Openssl still has the problems in the above content, in the past, even due to internal problems, the history of data leakage. In our selection, we still chose Openssl as the carrier of basic secure sockets, but at the same time we chose a custom internal standard algorithm to provide reliable transmission. The secure socket layer solution and communication architecture use OpenSSL as the basic dependency library for SSL development.

When Java uses OpenSSL, it needs to be called by JNI. In the standard JDK, it is only stipulated that JCE (Java Cryptography Extension) is a set of packages that provide a framework and implementation for encryption, key generation and negotiation, and Message Authentication Code (MAC) algorithms. It provides encryption support for symmetric, asymmetric, block and stream ciphers, and it also supports secure streams and sealed object interfaces. This article uses the following two ways to handle public and private keys: 1. Read by stream: Suitable for getting InputStream by indexing resources by ID in Android applications; 2. Read by string: As shown in the code, the key content is stored in static constants in rows, and the key is imported in String type.

In the actual Socket application development, these steps need to be inserted into the specific stage of Client/Server network communication. The flowchart of the SSL technology solution is shown in Figure 1.

![SSL Technology Flowchart](image-url)
3.2. Secure socket layer compensation scheme

The use of secure sockets improves the security of network transmission, and at the same time reduces the computing performance and network performance of the device. This article does not use http-like application layer protocols, but chooses to use a custom application layer protocol, and can freely choose the underlying use TCP still supports disconnected UDP.

3.2.1 Compensation for resource occupation

Compared with TCP, UDP is more flexible and efficient, and supports disconnection, that is, end-to-end communication connection when needed, otherwise it will not occupy connection resources. The connection is occupied when sending data, and it is disconnected after the data is sent. Therefore, a solution is adopted to compensate the performance loss for SSL resource occupation:

1. The UDP protocol that supports disconnection can reduce the occupation of server system network resources. The schematic diagram of TCP and UDP transmission mode is shown in Figure 2.

![Figure 2. TCP and UDP modes in TCP/IP](image)

The schematic diagram of TCP and UDP transmission and utilization is shown in Figure 3:

![Figure 3. Transmission resource utilization of TCP/IP and UDP](image)

2. Data compression. The use of SSL-encrypted data will greatly increase the length of data packets sent on the network, which will increase the network transmission time. Using data packet compression will increase the additional overhead of the CPU. Therefore, choosing an efficient algorithm can not only meet the additional performance loss, but also reduce the Data packet volume.

3. SSL offloading. Put a dedicated SSL application on the front end of the server without affecting the CPU and additional network resources of the background server, thereby
completely eliminating the load of SSL data processing.

3.2.2 Data loss compensation
Under the premise of limited network resources, UDP can provide the largest communication request. However, in the case of network congestion, UDP cannot perform flow control to avoid network congestion, such as packet loss during transmission, or the order of arrival and delivery of packets is disordered. Therefore, it is necessary to design a reliable protocol for control. The specific technical indicators of the compensation scheme are described as follows:

(1) Congestion control: In order to make better use of network resources, it is forbidden to send more data than the bandwidth allowed by the server, so it is necessary to set the maximum bandwidth control to prevent a large amount of data from being stuck in insufficient bandwidth and causing congestion. This situation may lead to buffer overflow, and the network load is not as good as the corresponding situation. Therefore, it is very necessary to control the bandwidth occupation.

(2) Load identification and QoS: In a fluctuating network environment, only static variables are used to set bandwidth utilization and sometimes the actual bandwidth and traffic cannot be well controlled. Therefore, it is necessary to dynamically monitor the network load and identify the maximum egress bandwidth to achieve dynamic control. At the same time, UDP itself does not provide any mechanism to ensure real-time delivery and provide other service quality QoS, but rely on the underlying services to complete. Therefore, it is very important to develop a QoS service.

(3) Data packet sequence: When using UDP to send data, the data packets are serialized. When these data packets are received and arrive in the order of transmission, the sequence number can be used to identify the order to rearrange the order of the data packets. Otherwise, the arriving data may be abnormal.

(4) Timestamp and monitoring: Timestamp is generally used for network streaming media. In ordinary data transmission, it can also be used to determine the time of data transmission and reception. At the same time, the data arriving at the same time is always monitored. If the monitoring finds packet loss, the server will be notified to resend. Larger jitter informs the server to slow down the sending rate.

4. Data encryption algorithm technology

4.1. Non-standard development of AES symmetric algorithm
The mainstream data encryption algorithm and fingerprint digest algorithm, and use this as a prototype to analyze and build a standard-based privatization algorithm that does not follow the standard, so as to ensure the uniqueness of the algorithm and the irreversibility of the result. The technical solutions mentioned in the article can be applied to the informatization development of a variety of enterprises and institutions with high security requirements, and to improve the security of data. The symmetric encryption algorithm is relatively simple, while the AES algorithm is more efficient than DES, the encrypted data is more secure, and the cracking cost is greater. As the encryption algorithm replacing DES, AES is the block encryption standard used by the US Federal Government. Compared with DES, it is more secure and efficient. Various industries around the world use AES as the basic encryption algorithm in a wide range of fields. As of 2006, AES has become one of the most popular algorithms in symmetric key encryption worldwide.

AES has three encryption features: 1. It can resist known attacks to the greatest extent; 2. It has nothing to do with the platform, the efficiency of encryption and decryption is fast, and the codec is compact; 3. Simple design. Therefore, choosing AES has a more reliable data encryption scheme without losing too much terminal and server performance. In AES, obfuscating the key decentralization is the basic design basis of the cipher block algorithm. To defend against potential linear attacks and known plaintext metadata, the key of the design is not to set the length of the key.
An important part of AES is the definition of S-box. In the S box, a new byte is mapped to each byte, and the high and low bits of the byte are assigned in rows and columns. Then get the corresponding row and column elements in the S box as output. The S box is a byte matrix composed of 16 * 16, containing 256 possible transformations that can be expressed by an eight-bit value.

4.2. Non-standard development of MD5 fingerprint digest algorithm

The MD5 algorithm also avoids the use of standard algorithms or language integration algorithms to avoid the possibility of fingerprints being tampered with. In this way, double security from data to fingerprint is realized. If you want to ensure the safety, efficiency, and integrity of the workshop management system and the informatization data and communication of industrial equipment. The above-mentioned method can minimize the occupation of system resources and provide reliable communication guarantee, as well as data security and integrity. Therefore, the same technical means as AES are used to prevent MD5 from obtaining data through dictionary mapping. As one of the irreversible algorithms, MD5 has the characteristics of high anti-collision, but as a general and open standard algorithm, choosing open source or language built-in algorithms during development will greatly compromise the security of the system. The open source algorithm and the algorithm that comes with the language are used by the most developers because of their openness, and the most fingerprint dictionaries are also produced. In theory, MD5 is irreversible, but because of its general characteristics, there are already many MD5 fingerprint mapping databases. Therefore, it is easy to obtain metadata through data dictionary mapping and comparison, so custom algorithm implementation details are necessary means.

The simple description of MD5 algorithm can be divided into: Use 512 as the packet to process the input data, where each packet is divided into 16 sub-packets of 32 bits. After processing, the algorithm outputs four 32-bit arrays. Then concatenate these four 32-bit packets into a 1278-bit hash value data. There are four 32-bit integer parameters called Chaining Variables in MD5. They are: A = 0x01234567, B = 0x89abcdef, C = 0xfedcba98, D = 0x76543210. After setting the four variables, it starts to enter the four-round loop operation of the algorithm. The number of loops is the count of 512-bit data packets in the data. Copy the above four variables to the target variable, respectively A-a, B-b and so on. Each operation performs a nonlinear function operation on three of a, b, c, d. Then add a fourth variable to the result. Examples of nonlinear functions are as follows:

- \( F(X,Y,Z) = (X \& Y) | (\neg X \& Z) \)
- \( G(X,Y,Z) = (X \& Z) | (Y \& \neg Z) \)
- \( H(X,Y,Z) = X^Y^Z \)
- \( I(X,Y,Z) = Y^(X|\neg Z) \)

The custom algorithm can change the filling order inside the nonlinear function to make it confusing. The bitwise operators of subgroups can also be confused by transposition. Suppose \( M_j \) represents the jth subgroup of the message (from 0 to 15):

- \( FF(a,b,c,d,M_j, s, ti) = a = b + ((a + F(b,c,d) + M_j + ti) \ll s) \)
- \( GG(a,b,c,d,M_j, s, ti) = a = b + ((a + G(b,c,d) + M_j + ti) \ll s) \)
- \( HH(a,b,c,d,M_j, s, ti) = a = b + ((a + H(b,c,d) + M_j + ti) \ll s) \)
- \( II(a,b,c,d,M_j, s, ti) = a = b + ((a + I(b,c,d) + M_j + ti) \ll s) \)

Then take the first round of filling as an example in the four rounds of circular operation as follows:

- \( FF(a,b,c,d,M0,7,0xd76aa478) \)
- \( FF(d,a,b,c,M1,12,0xe8c7b756) \)
- \( FF(c,d,a,b,M2,17,0x242070db) \)
- \( FF(b,c,d,a,M3,22,0xc1bdceee) \)
- \( FF(a,b,c,d,M4,7,0xf57c0faf) \)
- \( FF(d,a,b,c,M5,12,0x4787c62a) \)
- \( FF(c,d,a,b,M6,17,0xa8304613) \)
- \( FF(b,c,d,a,M7,22,0xf469501) \)
- \( FF(a,b,c,d,M8,7,0x698098d8) \)
Through the above demonstration, we know the basic method and process of MD5 fingerprint calculation, so we can achieve the privatization of the MD5 algorithm in the following two ways:

1. Modify the permutation array combination, for example: \( FF(a,b,c,d, x[0], S11, 0xd76aa478) \), modify it to \( FF(a,b,c,d, x[0], S11, 0xd12aa123) \); or change the filling order of a\( \equiv \)b\( \equiv \)c\( \equiv \)d.

2. Modify the output byte sequence. Through the above technical means, the encryption result of the MD5 algorithm will be completely different from the result produced by the standard and open source libraries, so as to prevent the data from being cracked by dictionary collision.

4.3. Network communication secure socket and data double encryption scheme

This security information management system uses AES, MD5 and SSL triple security technology. Used to ensure that data transmission is not disguised, tampered with and monitored. The scheme for sending encrypted data is as follows:

After the system accepts the data entered by the user, it is restricted to use AES to encrypt the input metadata, and then use MD5 to perform fingerprint verification on the encrypted data, and then format the encrypted metadata and MD5 fingerprint data into the message protocol and then pass the data through SSL secure socket for transmission. In this case, the correct data cannot be obtained even after SSL is broken, and the custom AES and MD5 algorithms ensure that even if the metadata is obtained and sent in disguise, it cannot be achieved because there is no original encryption algorithm and key. Even if the metadata is obtained, the plaintext cannot be obtained. The replaced data cannot generate the fingerprint we want. Therefore, if the metadata is replaced, it may not be able to be read and parsed normally. The consequences of replacing the fingerprint are the same. For a fingerprint that cannot be read correctly, we can fundamentally judge that the data is invalid or incomplete.

From the above figure, we can see that after the data is received, we will not directly decrypt the data, but will calculate whether the metadata fingerprint is the same as when it was sent. If the fingerprint is wrong, we will not proceed to the next step. The detailed process is shown in Figure 4:

---

**Figure 4.** Multi-security protection network security process
5. Conclusion
The main goal of this paper is to solve the hidden dangers of the existing information security management system, and the innovation point is the security process and mode. The security expansion of the security management system based on multiple encryption technologies is just a microcosm of information security. This article provides a reliable information security solution that can also be applied to other scenarios.

6. References
[1] Fan N N 2016 Research and Application of "Internet + Intelligent Manufacturing" Technology Architecture. Soochow University.
[2] Jin J 2016 Research on the transformation and upgrading of China's manufacturing industry in the era of Industry 4.0. Yunnan University.
[3] Chen J Y 2015 Research on the planning and construction of an enterprise's deep integration of informatization and industrialization based on the idea of Industry 4.0. Zhejiang University of Technology.
[4] Jiang X F 2015 Application research of Android white box encryption. Xidian University.
[5] Sun C 2015 Research on the security of embedded database based on smart devices. Jilin University.
[6] Cai X W 2015 Research and design of database encryption technology based on C/S structure. Guangdong University of Technology.
[7] Tan J 2015 Optimization and application of IDEA encryption algorithm based on Android platform. Nanchang University.
[8] Chen Q C 2015 A hybrid encryption algorithm based on DES and RSA algorithms. Yunnan University.
[9] Reliability of manufacturing equipment in complex environments. Jeffrey P.Kharoufeh,Steven M.Cox,Mark E.Oxley. Annals of Operations Research. 2013(1).
[10] Failure Mode Effects and Criticality Analysis (FMECA) of Circular Tool Magazine and ATC. Xiaohong Lu,Zhenyuan Jia,Shengnan Gao,Pengzhuo Han. Journal of Failure Analysis and Prevention. 2013 (2).
[11] Optimal maintenance schedule decisions for machine tools considering the user’s cost structure. BhupeshKumar Lad,MakarandS. Kulkarni. International Journal of Production Research. 2012 (20).