Information and Knowledge Management (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/infkm.2022.030201
ISSN 2523-5893 Vol. 3 Num. 2

Exploring the Application of Data Encryption Technology in Computer Network Security

Junling Li

Jining Normal University, Ulanqab, Inner Mongolia, China
Ljl_rr@163.com

Keywords: Data Encryption Technology, Computer, Network Security

Abstract: This paper starts from the current situation of computing network security, introduces the types of data encryption technology and algorithms, explores in depth the application of data encryption technology in computer network security, and strengthens its role in the maintenance of network information security, in order to provide a good network environment for users.

With the continuous development of computer network technology, it has become a reliable technology for transmitting and storing huge amount of data in production and life practice. However, due to the characteristics of openness and sharing of network environment, the security problems of data transmission and storage are becoming more and more prominent, and how to guarantee network information security has become the main research direction in this field. As an important technology to protect computer network information security, data encryption technology is of great practical significance to prevent data loss, leakage and tampering, and to guarantee the stability and confidentiality of data in transmission and storage[1].

1. Overview of Data Encryption Technology

1.1. The Meaning of Data Encryption Technology

Data encryption technology is a technical means to protect the security of computer network information. It uses the principle of cryptography technology to encrypt the transmitted data and apply the encryption function to replace and shift the data, so as to protect the data from being stolen in the transmission, and when the data is transmitted to the receiving end, the decryption key is used to restore the ciphertext information. In the process of data transmission, data encryption, data transmission, and data decryption are experienced, which effectively improves the concealment of data information transmission and maintains the security of computer network operation[2].

1.2. Algorithm of Data Encryption Technology

First, the transposition table algorithm. It is the simplest encryption method among the encryption algorithms, which is to output each data segment with different offsets in the transposition table, and then form an encrypted file with the values corresponding to the offsets, and when the data is transmitted to the receiver, the decryption program only needs to refer to the transposition table to finish decoding the cipher text. The encryption and decryption process of the permutation table algorithm is simple and the encryption and decryption speed is fast, but if others get access to the transposition table. However, if someone else gets access to the substitution table, they will recognize the encryption scheme and decipher the secret text directly.

Second, the improved permutation table algorithm. The improvement of the above replacement table method is to use two or more replacement tables to encrypt the data information in a random way using the replacement table, which makes it more difficult to decipher the cipher text and thus improves the security of the data information. Even if a hacker obtains the plain text and cipher text, it is still very difficult to decipher the encryption scheme.

Third, cyclic shift and XOR operation algorithm. Cyclic shift is to shift a word or byte within a data stream cyclically to the left or right to change the data position and generate a new data stream, and then apply XOR operation algorithm to complete the encryption and generate the cipher text, which is difficult to be deciphered directly[3]. If we further use XOR operation to do a bitwise heterogeneous operation, it will be more difficult to decipher the cipher text, which enhances the security of data transmission.

Fourth, cyclic redundancy check algorithm. This is a commonly used check algorithm with strong error detection capability. When data is transmitted to the computer at the receiving end, the cyclic redundancy check algorithm is used to detect or check the accuracy of the digital transmission on the communication link. In the cyclic redundancy check algorithm, for each piece of network data, a 16-bit or 32-bit checksum is generated using a bit-cycle shift and XOR operation. When data is lost or an error occurs, it will result in an error in the final checksum, which indicates that there is an error in the data sent, and the receiver can request the sender to resend the data. This kind of encryption algorithm can complete the calculation of data checksum in a very short time and complete the error correction process quickly, with high communication efficiency, strong error detection ability and low detection cost, so it is widely used in the field of data transmission[4].

1.3. Types of Data Encryption Technology

1.3.1. Symmetric encryption technology

Symmetric encryption technology means that the receiver and sender share the same key during the transmission of information, and negotiate to use the same key for encryption and decryption when sending and obtaining information, which requires that both parties need to deliver the ciphertext in a secure transmission environment during the transmission of information. The advantages of symmetric encryption algorithm are simple computation process, open algorithm, high operation efficiency and fast encryption speed[5]. The disadvantages are that the sender and receiver of data must agree and keep the secret key, and if one party's key is leaked, the encrypted message cannot be secured. Moreover, each data transmission needs to use a unique key, which will make the number of keys owned by both parties huge and the key management becomes a burden. The commonly used symmetric encryption algorithms are DES, AES, etc. Among them, DES algorithm is group encryption technology, the length of the key is 64 bits, 8 bytes, which can be suitable for encryption processing of a large amount of data and runs faster. AES key length is 128, 192 and 256 bits, which is 16 bytes, 24 bytes and 32 bytes, the algorithm is faster than DES, and at the same time, it improves the effective utilization of resources, and has become a standard encryption algorithm.

1.3.2. Asymmetric Cryptography

Asymmetric encryption technology has two keys: public key and private key, the private key can only be kept by one party and cannot be leaked, and the public key can be given to any requesting party. In practical application, the two parties transmitting and receiving data need to encrypt and decrypt the data via different keys and functions, and the two parties communicating data do not need to exchange keys in advance; if the data is encrypted with public key, it can only be decrypted with the corresponding private key; if the data is encrypted with private key, it can only be decrypted with the corresponding public key. Because two different keys are used for encryption and decryption, this algorithm guarantees the confidentiality and security during data transmission, which is also the advantage of asymmetric encryption technology; the disadvantage of asymmetric encryption technology is that the operation efficiency is low and it is not suitable for fast decryption. The commonly used asymmetric encryption algorithms are DSA, RSA, ECC and so on. Among them, ECC is better than DSA and RSA in terms of encryption speed and storage space.

2. Security Risks Facing Computer Network Information

With the rapid development of information technology, computer networks have been fully applied in all walks of life, and people are facing serious computer network information security problems while enjoying the efficiency and convenience brought by computer networks, such as data being leaked, tampered with or lost in the transmission process, and so on. The factors that lead to computer network information security problems are mainly the following.

2.1. Hacking

With the continuous diversified penetration of Internet technology in all walks of life, the security of computer network information in the process of transmission and storage is facing a great challenge. According to statistics, most of the data in computer data management systems are tampered with or stolen due to hackers invading computer systems through illegal means and breaching firewalls, making computer network data security under great threat. Hacker's attack is an active behavior, usually for a certain purpose to take illegal means to invade the computer system, malicious damage to data information, so that people's lives and property face incalculable losses. Therefore, it is necessary to strengthen the protection of computer data and information management system, and put the maintenance of computer network data security in an important position.

2.2. Computer Network Vulnerability

The IP protocol security performance of some computer networks is relatively low, which gives an opportunity for lawless elements to invade computers. Lawless elements use various network vulnerabilities to transmit virus source file packages to computer systems, and further transmit virus source files to various computer software under the influence of network vulnerabilities, resulting in data information being tampered with or lost, and even affecting the normal operation of computer network systems. Another network vulnerability is the lack of a standardized network management system and management standards in the computer industry, and the lack of regular inspection and maintenance work during the operation of the network, resulting in certain security risks of network information.

2.3. Virus Software

Virus software is an artificially prepared code used to destroy computer functions and data, which is highly contagious, hidden, latent, and triggered. With the help of computer network loopholes, virus software spreads and replicates rapidly, causing great damage to computer networks and data. For example, the Internet is filled with a large number of Trojan horses, macro viruses, worms, which are often attached to low-security Web sites or files, once the user triggers a certain condition will stimulate the virus to attack or damage the system, and the computer shares a network with the computer will be infected by the virus, resulting in a large area of computer paralysis, making it difficult for the computer network to operate normally.

3. The Use of Data Encryption Technology in Computer Network Security

3.1. Link Encryption Technology

Link refers to the channel composed of each node in the process of data transmission. Link encryption means that the data existing in the network hierarchy is first encrypted so as to guarantee the security between nodes in the process of data transmission, and each node in the link decrypts the received data, and then uses the key of the next link to encrypt the data twice so as to implement effective transmission of data.Before reaching the target computer, data may need to be encrypted, transmitted and decrypted several times, ensuring the security and accuracy of data information. By maintaining the channels composed of each node, link encryption makes data information pass in the form of cipher text to guarantee the security during data transmission of each link, and it can also encrypt the address information of the sending end and the receiving end to effectively avoid the loopholes existing in end-to-end encryption. Moreover, the integration of padding technology and link encryption technology can further improve the security of link encryption technology. However, in the process of data transmission, link encryption requires multiple decryption and encryption operations, which makes the link transmission process tedious and complicated and affects the propagation efficiency, and it is not easy to deal with encryption problems once they occur.

3.2. Node Encryption Technology

In the process of network information transmission, the data has to go through a series of network nodes to finally reach the target computer, in which the data will be maliciously attacked and damaged by computer viruses and unscrupulous elements. Node encryption technology refers to encrypting the data for transmission first, decrypting the data at the intermediate nodes, and then encrypting it again using different keys before finally transmitting to the target computer. During the data transmission, the nodes must ensure the security of the module to be implemented, and the data is not allowed to exist in plaintext form at the network nodes. Node encryption technology is applied to decrypt and re-encrypt the data of each node, which can strengthen the security of data transmission and enhance the protection of computer network data.

3.3. End-to-end Encryption Technology

End-to-end encryption technology is to encrypt data information according to certain rules or algorithms, then transmit the cipher text in the network, and decode it after all the cipher text has been transmitted. Even if the node is attacked or damaged during the data transmission, the data information will not be stolen, and this encryption technology can better guarantee the security of data information transmission. Compared with other encryption technologies, end-to-end encryption technology eliminates the decryption processing of data by intermediate nodes, and the number of decryption devices is relatively small, which greatly saves equipment cost and transmission time.

Compared with node encryption technology and link encryption technology, end-to-end encryption technology is simpler, can effectively save cost and time, and has better stability in data transmission, so end-to-end encryption technology is widely used in network security maintenance work. However, it also has disadvantages. End-to-end encryption technology can only encrypt the information of the message, but not the data information of the header, and the security of data transmission is insufficient, so we can only decide whether to use end-to-end encryption technology according to the needs of users.

4. Conclusion

The rapid development of Internet technology makes the network security problem more and more prominent, and data encryption technology is the main technology to ensure the security of computer networks. According to different network environments, different data encryption technologies are chosen to effectively prevent the loss, leakage and tampering of network data, and provide strong support and guarantee for the safe and orderly operation of computer networks.

References

[1] Aghili Seyed Farhad, Sedaghat Mahdi, Singelée Dave et al. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme [J]. Future Generation Computer Systems, 2022, 131.

[2] Xiang Xinyin, Zhao Xingwen. Blockchain-assisted searchable attribute-based encryption for e-health systems [J]. Journal of Systems Architecture, 2022(124-):124..

[3] Huang Fengming, Waqas Muhammad, Tu Shanshan et al. A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing [J]. Computer Networks, 2020, 46(5):7.

[4] Patil S , Patil S S , Solunke B R . Literature review on Efficient and Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems[J]. 2015(4).

[5] Nagulmeera S , Imran M . Protect Revocable Data Access Control for Multi-Authority Cloud Storage. 2015.