ISSN 2616-5775 Vol. 6, Issue 10: 43-47, DOI: 10.25236/AJCIS.2023.061007

Application of Data Encryption Technology in Computer Network Security

Olric Yuhang Zeng

Troy High School, Los Angeles, US

Abstract: *With the rapid development of computer technology, computer network security is an important issue that cannot be ignored in modern society, and data encryption technology plays a key role in ensuring the security of computer network. As one of the important means of computer network security, data encryption technology is widely used to protect sensitive information. Data encryption technology plays an important role in computer network security and needs to be continuously studied and explored to meet the increasingly severe challenges of network security. This paper will discuss the classification, advantages and application of data encryption technology in computer network security, and discuss the application of data encryption technology in computer network security.*

Keywords: *Data encryption technology; Computer network security; Application*

1. Introduction

Data encryption technology is an important part of computer network security, it can effectively protect the confidentiality, integrity and availability of data. In computer networks, data encryption technology is widely used in data transmission, storage and access control. With the continuous development of network technology, data encryption technology will face increasing challenges. Therefore, future research should focus on developing more efficient and secure data encryption algorithms and techniques, while strengthening key management and security protocols. In addition, it is necessary to improve people's awareness of network security and strengthen network security education to jointly maintain a safe network environment.

2. Classification of Data Encryption Technology

Data encryption technology refers to the process of transforming plaintext information into ciphertext through a certain algorithm. The ciphertext can only be decrypted and restored to plaintext with the corresponding key. The core elements of data encryption technology are the algorithm and the key, where the algorithm is the specific process of converting plaintext into ciphertext, and the key is the critical factor ensuring the security of encryption and decryption.

Data encryption technology can be classified into symmetric encryption and asymmetric encryption based on different encryption methods.

2.1. Symmetric Encryption

Symmetric encryption refers to the encryption and decryption using the same key. The same key is used for both encryption and decryption, resulting in faster encryption speeds. However, attention must be paid to key management and distribution issues. Common symmetric encryption algorithms include DES, 3DES, AES, etc.[1]

2.2. Asymmetric Encryption

Asymmetric encryption refers to the encryption and decryption using different keys. Public key is used for encryption, while private key is used for decryption. Asymmetric encryption algorithms provide higher security, but encryption and decryption speeds are slower, due to the time it takes to run the plaintext through mathematical equations to encode and decode them. Common asymmetric encryption algorithms include RSA, DSA, etc.

ISSN 2616-5775 Vol. 6, Issue 10: 43-47, DOI: 10.25236/AJCIS.2023.061007

3. Advantages of Data Encryption Technology in Computer Network Security

3.1. Preventing Data Leakage

Data leakage is a serious issue in today's digital world, involving the unauthorized disclosure of sensitive data to third parties. Various sectors, including banking, healthcare, education, and government, deal with a vast amount of sensitive data. Therefore, effectively preventing data leakage and safeguarding the security of sensitive data have become crucial tasks we currently face.

Firstly, it is important to understand the severity of data leakage. Data leakage can lead to the exposure of personal privacy and business secrets, causing significant losses to individuals, organizations, and even entire countries. The leakage of personal information can result in privacy infringement and even lead to identity theft and other criminal activities. The leakage of business secrets can weaken a company's competitiveness and even threaten its existence. The leakage of sensitive information at a national level can pose a threat to the country's security.[2]

To prevent data leakage, data encryption technology can be employed. Data encryption is an effective measure to prevent data leakage by transforming data into an encrypted form, making it inaccessible to unauthorized parties even if the data is stolen. This can effectively protect the security of personal privacy and business secrets, ensuring the safety of individuals, organizations, and countries.

Data encryption technology comes in various forms, including symmetric encryption, asymmetric encryption, and obfuscation. Symmetric encryption involves using the same key for both encryption and decryption, such as DES and AES. Asymmetric encryption, on the other hand, uses different keys for encryption and decryption, like RSA and ECC. Obfuscation refers to altering the structure and code of a program to make it difficult for attackers to understand and analyze, thus protecting the data.

In practical applications, we can choose appropriate data encryption technology based on specific data types and protection requirements. For instance, for sensitive data stored in databases, we can utilize database encryption technology to store data in an encrypted form, ensuring its security. For data transmitted during communication, we can use transport layer security technologies like SSL/TLS to encrypt data during transmission, preventing data theft in transit.

3.2. Preventing Data Tampering

Data tampering is a serious security issue where attackers make unauthorized modifications to the original data during data transmission or storage. This situation may compromise data integrity, affecting its reliability and credibility, and could even lead to severe consequences such as decision errors, business interruptions, or reputational damage.

To prevent data tampering, various measures can be taken, with one of the most important being the use of data encryption technology. Data encryption ensures the integrity and confidentiality of data during transmission and storage. By encrypting the original data and generating ciphertext, even if attackers intercept the ciphertext, they cannot obtain the correct decryption key to decrypt the original data properly. Therefore, attackers cannot effectively use the tampered data.

In addition to data encryption, other technologies can also help prevent data tampering, such as using hash functions and digital signatures. Hash functions can convert arbitrary-length inputs (also known as messages) into fixed-length outputs, known as hash values or message digests. Due to the properties of hash functions, even minor modifications to the input will result in significant changes to the output hash value.[3] Therefore, we can compare the hash values of data to check for data tampering.

Digital signatures are another technology used to prevent data tampering, combining hash functions with public-key encryption. When sending data, the sender first calculates the hash value of the data and then encrypts the hash value using their private key to generate a digital signature. Upon receiving the data and signature, the receiver can decrypt the signature using the sender's public key to obtain the hash value, then calculate the hash value of the received data and compare the two hash values to verify the data's integrity.

ISSN 2616-5775 Vol. 6, Issue 10: 43-47, DOI: 10.25236/AJCIS.2023.061007

3.3. Enhancing Data Security

Data encryption technology is a technique that transforms original data (plaintext) into unreadable data (ciphertext) using specific encryption algorithms and keys. Its purpose is to prevent unauthorized individuals from accessing and understanding sensitive information. As encryption is a reversible process, we can use the correct key to decrypt and restore the original plaintext data when needed. Encryption technology has become a crucial means of ensuring data security, particularly in areas involving sensitive information such as personal privacy, trade secrets, or national security.

Protecting Data Confidentiality: Encrypted data cannot be understood directly by individuals without the encryption key. Even if the data is intercepted during transmission or accessed illegally during storage, attackers cannot access the actual data content.

Protecting Data Integrity: Many encryption algorithms, such as public-key encryption, can be used not only to encrypt data but also to generate digital signatures for verifying data integrity and sources. By comparing the received data with the digital signatures, we can check whether the data has been tampered with during transmission.

Ensuring Data Availability: Encryption technology prevents data from being unlawfully tampered with, ensuring data availability. Even if attackers can tamper with the encrypted data, they cannot generate the correct digital signatures, leading the receiving party to identify and reject the tampered data.

In practical applications, key management and access control are also crucial aspects. A sound key management strategy ensures the security of keys, preventing key loss or leakage. Access control prevents unauthorized individuals from accessing sensitive data, further enhancing data security.

3.4. Preventing Hacker Attacks

Hacker attacks pose a serious security threat that can lead to data breaches, system crashes, business interruptions, and other severe consequences. Moreover, as technology advances, the forms and methods of hacker attacks continue to evolve and escalate, placing higher demands on the security of our data and systems. To effectively prevent hacker attacks, we need to implement a series of technical and managerial measures, among which data encryption technology plays a crucial role.

Data encryption technology can protect data security and prevent hackers from stealing or tampering with data during transmission and storage. This mainly relies on the security of encryption algorithms and keys. Only those with the correct key can decrypt and access the original data. Otherwise, even if the data is stolen, attackers cannot understand or use the data. This significantly reduces the risk of data leakage and enhances data security.

Additionally, access control and key management are important measures to prevent hacker attacks. Access control prevents unauthorized users from accessing and operating sensitive data within the system, ensuring that only authorized users can access and manipulate data, thus preventing the possibility of data misuse. Key management ensures the security of keys, preventing key loss or leakage, and ensures that only authorized users can use the keys, further enhancing system security.

Furthermore, conducting regular security audits and vulnerability scans on the system to promptly fix discovered security vulnerabilities and risks is also an essential measure to prevent hacker attacks. Additionally, educating and training users to enhance their security awareness and skills are effective ways to prevent hacker attacks.

In conclusion, data encryption technology offers advantages in preventing data leaks, data tampering, enhancing data security, and preventing hacker attacks. By using data encryption technology, the security of sensitive data such as personal privacy and trade secrets can be ensured, thereby safeguarding individuals, organizations, and countries. Additionally, to ensure the effectiveness of encryption technology, attention should be given to the security aspects of encryption algorithm selection and key management to prevent security risks such as hacker attacks and data leakage.

ISSN 2616-5775 Vol. 6, Issue 10: 43-47, DOI: 10.25236/AJCIS.2023.061007

4. Application of Data Encryption Technology in Computer Network Security

4.1. Network Communication Encryption

Network communication encryption refers to encrypting data during its transmission over the network to protect it from being intercepted or tampered with. In network communication, data transmission often involves multiple nodes, which may have security vulnerabilities. Therefore, for sensitive data, encryption technology is used to ensure protection.

Network communication encryption is mainly achieved through the use of encryption protocols, with SSL (Secure Sockets Layer) and TLS (Transport Layer Security) being common encryption protocols for network communication. SSL and TLS are widely used protocols that ensure the security of data during transmission.[4]

The SSL protocol uses public and private keys for encryption. In the SSL protocol, the server needs to use a digital certificate to verify its identity and provide the public key to the client. The client uses this public key to encrypt data before sending it to the server, which then decrypts it using its private key. This process ensures that the data remains secure during transmission. TLS is an improved version of the SSL protocol, offering better security and performance.

4.2. File Encryption

File encryption involves encrypting files so that only authorized users can view their contents. This technique is commonly used to protect sensitive data like business secrets and personal privacy. By using file encryption, it prevents unauthorized access or leakage of files.

File encryption can be achieved using either software or hardware. Common file encryption software includes TrueCrypt and VeraCrypt, which use passwords to encrypt files, allowing only users with the correct passwords to view the file contents. Hardware encryption, on the other hand, utilizes hardware modules to encrypt files, offering higher security and performance.

4.3. Database Encryption

Database encryption refers to encrypting the data stored in a database to protect its security. Data stored in databases often contains sensitive information such as business secrets and personal privacy, making encryption technology crucial for protection.

Database encryption technology can be implemented using software or hardware. Common database encryption technologies include TDE (Transparent Data Encryption), Oracle Database Vault, etc. TDE technology enables encryption of data within the database, ensuring the security of data during storage. Oracle Database Vault is a role-based access control technology that controls user access to data in the database, thereby ensuring data security.

4.4. Hard Disk Encryption

Hard disk encryption refers to encrypting the entire hard disk to protect the data stored on it. Hard disk encryption technology effectively prevents data leakage when the hard disk is lost or stolen.

Hard disk encryption can be implemented using software or hardware. Common hard disk encryption technologies include BitLocker, FileVault, and others. These technologies encrypt the entire hard disk, and only users with the correct password or encryption key can access the data on the hard disk. Hard disk encryption provides higher security and reliability, ensuring the security of data during storage.

In conclusion, data encryption technology plays a crucial role in computer network security. By using encryption technology, sensitive data can be protected, preventing data theft or tampering. Different encryption technologies can be applied to various scenarios, such as network communication encryption, file encryption, database encryption, and hard disk encryption. It is essential to choose the appropriate encryption technology based on specific requirements to safeguard data security. Additionally, to ensure the effectiveness of encryption technology, attention should be given to the security aspects of encryption algorithm selection and key management to prevent security risks like hacker attacks and data leakage.

ISSN 2616-5775 Vol. 6, Issue 10: 43-47, DOI: 10.25236/AJCIS.2023.061007

5. Conclusion

Data encryption technology is one of the essential means in computer network security, effectively protecting data security. It can be applied in various areas such as network communication encryption, file encryption, database encryption, and hard disk encryption, safeguarding the security of personal privacy and business secrets. Compared to other security technologies, data encryption technology has higher security and reliability, making it a crucial method for ensuring computer network security. Therefore, the application prospects of data encryption technology are extensive in the fields of computer network security and communications.

References

[1] Ji Qianqian. Discussion on the Application of Data Encryption Technology in Computer Network Security. Network Security Technology and Applications, 2023(07): 22-23.
[2] Liu Yang. Application of Data Encryption Technology in Network Security Transmission. Cyber Space Security, 2023, 14(03): 41-44.
[3] Liu Zhenhua. Analysis of Data Encryption Technology in Computer Network Information Security. Digital Communication World, 2023(06): 67-69.
[4] Zhang Mei. Application of Data Encryption Technology in Computer Network Information Security. Journal of Jiamusi Vocational College, 2022, 38(12): 152-154.