e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

A REVIEW PAPER ON NETWORK SECURITY AND CRYPTOGRAPHY

Sachin Ade[*1], Shadab Khan[*2], Kedar Kannao[*3], Gopal Gawande[*4],
Mahesh Rathod[*5], Prof. V.R. Thakare[*6]

[*1,2,3,4,5]Final Year Student,Electronics& Telecommunication Jagadambha College Engineering & Technology Yavatmal, Maharashtra, India.

[*6]Guide, Electronics& Telecommunication Jagadambha College Engineering & Technology Yavatmal, Maharashtra, India.

ABSTRACT

With the rise of the World Wide Web and the proliferation of e-commerce platforms and social networks, organizations worldwide are generating vast volumes of data on a daily basis. Ensuring the secure transmission of this data over the internet has become a paramount concern, making information security a fundamental issue. Additionally, as society transitions into the digital information age, network security has gained increasing importance. With a growing number of users connecting to the internet, the threat of cyberattacks has intensified. Consequently, safeguarding computer and network security has become imperative, addressing critical issues in the process. Malicious nodes in the network pose a significant challenge, as they can exploit the resources of other nodes while also protecting their own assets. This paper aims to provide an overview of network security and explore various techniques for enhancing it, particularly focusing on cryptography.

Keywords: Security, Vulnerabilities, Cryptographic Methods, Encoding, Deciphering

I. INTRODUCTION

The rapid advancement of modern internet and information technology has led to increased connectivity of individuals, businesses, educational institutions, and government departments to the internet. Consequently, this has attracted a surge in illicit users who employ tactics like fake websites, deceptive emails, Trojan horses, and backdoor viruses to launch attacks and disrupt networks. The primary targets of these attacks are computers, and once infiltrated, they can render thousands of networked computers inoperative. Furthermore, malicious actors with ulterior motives often target military and government entities, posing significant threats to social and national security .Cryptography, derived from the term "Hidden Secrets," revolves around the concept of encryption and secure communication. It plays a crucial role in studying protocols associated with various aspects of information security, including authentication, data confidentiality, data integrity, and non-repudiation. Cryptography is the art of encoding messages in secret code and involves designing and analyzing protocols to thwart adversaries. It addresses essential elements of modern information security, ensuring data remains confidential, intact, and authenticated .A key challenge lies in the effective sharing of encrypted data.

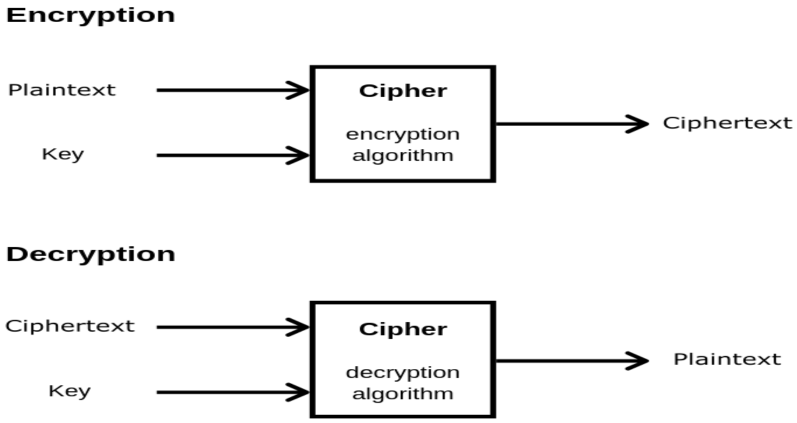


Fig.1. Plaintext & ciphertext

The process involves encoding messages with a securely shared key known only to the sender and recipient, a critical aspect for achieving robust security in sensor networks. Secure key exchange between the sender and recipient presents a significant challenge in resource-constrained sensor networks. In such networks, data should be encrypted by users before outsourcing it to remote cloud storage services. Both data security and data access security must be guaranteed to the extent that cloud service providers cannot decipher the data. Moreover, when users need to search specific segments of the encrypted data, the cloud storage system should provide accessibility without revealing the content of the returned data segments. This paper explores various approaches to network security and cryptographic methodologies.

II. LITERATURE REVIEW

2.1 Network Security Model

The diagram in Figure illustrates the system security model. In this model, a message needs to be transmitted from one party to another through an Internet service. An intermediary may be responsible for distributing the confidential information to both the sender and the recipient while preventing any interference from competitors. When establishing a secure network, the following factors should be taken into account:

Confidentiality: This refers to ensuring that unauthorized parties cannot access the information.

Integrity: It guarantees that the data received by the recipient has not been altered or tampered with after being sent by the sender.

All security measures involve two components:

A modification of the data to be sent to enhance security. Messages should be encrypted with a key to obscure them from potential adversaries.

An encryption key used in conjunction with the modification to encrypt the message before transmission and decrypt it upon reception.

Security considerations come into play when it is essential or desirable to protect the transmission of information from a potential threat to its confidentiality, integrity, and more.

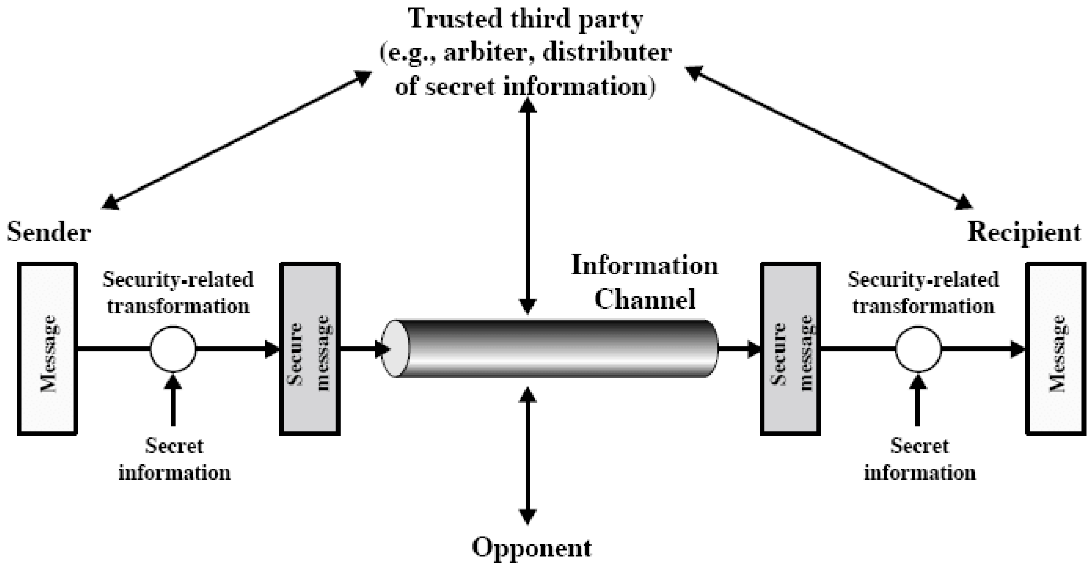


Fig.2. Network Security Model

2.2 Importance of Key Management in Cloud

Encryption provides data security, while effective key management enables access to protected data. It is highly recommended to encrypt data during transmission across networks, at rest, and on backup storage media. In particular, organizations should have the capability to encrypt their own data. Both encryption and key management are critical components for securing applications and data stored in the Cloud.

The requirements for efficient key management are outlined below:

Secure Key Stores: The key repositories themselves must be safeguarded against malicious users. If a malicious user gains access to the keys, they can potentially access any encrypted data associated with those keys. Therefore, key stores must be protected both physically and digitally, both during transmission and on backup media.

Access Control to Key Stores: Access to the key stores should be restricted to users who have the appropriate permissions to access the data. Role-based access control should be implemented to regulate access. The entity that utilizes a specific key should not be the entity responsible for storing that key. Key Backup and Recovery: Secure backup and recovery solutions for keys are essential. The loss of keys, although effective in preventing access to data, can be highly detrimental to a business. Cloud providers must ensure that keys are not lost due to issues with backup and recovery mechanisms.

III. CRYPTOGRAPHY MECHANISM

Cryptography is a method for storing and transmitting data in a specific format so that those for whom it is intended can read and process it. This term is often associated with the transformation of plaintext messages (common text, sometimes referred to as cleartext) into ciphertext (a process known as encryption) and then reversing it (referred to as decryption). Generally, there are three types of cryptographic schemes commonly used to achieve these goals: secret key (or symmetric) cryptography, public key (or asymmetric) cryptography, and hash functions, each of which is described below.

Key: A key can be a numeric or alphanumeric sequence or a unique symbol.

Plain Text: The original message that one person wishes to communicate to another is referred to as Plain Text. For example, if a person named Alice wants to send the message "Hi Friend how are you" to Bob, "Hi Friend how are you" is the plain text message.

Cipher Text: The message that cannot be understood by anyone or appears random is referred to as Cipher Text. For instance, "Ajd672#@91ukl8*^5%" is a Cipher Text generated for the message "Hi Friend how are you." Ciphertext is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the correct algorithm to decrypt it. Decryption, the reverse of encryption, is the process of transforming ciphertext into understandable plaintext. Ciphertext should not be confused with code text, as the latter is a result of a code, not a cipher.

Encryption: The process of converting plain text into cipher text is called Encryption. This process involves two components: an encryption algorithm and a key. The algorithm refers to the method used in encryption. Data encryption takes place at the sender's end.

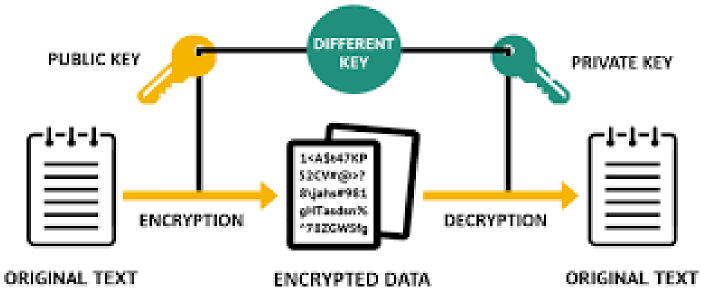
Decryption: The reverse process of encryption is called Decryption. In this process, cipher text is converted into plain text. The decryption process also requires two components: a decryption algorithm and a key. The algorithm refers to the method used in decryption. Generally, both algorithms are the same.

IV. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Encryption and decryption of protected data are typically achieved through two primary techniques: Asymmetric and Symmetric encryption.

Symmetric Encryption

In Symmetric Encryption, the same cryptographic keys are employed for both encrypting plaintext and decrypting ciphertext. Symmetric key encryption is characterized by its speed and simplicity. However, its primary drawback is that both users involved in communication must securely exchange their keys



A single key serves for both the encryption and decryption of data.

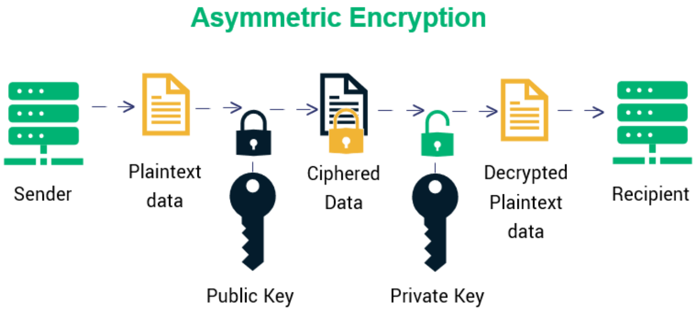
Types of Symmetric-Key Algorithms

Symmetric-key encryption employs either stream ciphers or block ciphers. Stream ciphers encrypt individual digits (typically bytes) of a message one at a time.

Block ciphers take a set number of bits and encode them as a single unit, padding the plaintext to match the block size. Historically, 64-bit blocks were common, but the Advanced Encryption Standard (AES) algorithm, approved by NIST in December 2001, and the GCM block cipher mode of operation employ 128-bit blocks.

Asymmetric Encryption

Asymmetric encryption, also known as Public Key Cryptography, utilizes two keys: a public key, known to the public, and a private key, known only to the user.



In Asymmetric key Encryption, two different keys are used for encryption and decryption:

The Public key and the Private key.

Public key encryption involves encrypting message data with a recipient's public key. The message cannot be decrypted by anyone lacking the corresponding private key, which is assumed to be owned by the key's holder. This approach aims to ensure confidentiality.

Digital Signature involves signing a message with the sender's private key and can be verified by anyone with access to the public key, enhancing network security.

AES (Advanced Encryption Algorithm)

AES is an iterated symmetric block cipher characterized by repeating a predefined set of steps multiple times. AES is a symmetric key encryption algorithm operating on fixed-size bytes. With the rapid growth of digital data exchange in electronic communication, data security has become increasingly vital. Cryptography plays a pivotal role in safeguarding information systems against various threats. Two cryptographic methods are utilized: symmetric and asymmetric. This paper focuses on the symmetric cryptographic technique AES (Advanced Encryption Standard), using 200-bit block size and key size, alongside the conventional 128-bit block size. The AES algorithm is implemented using a 5x5 matrix for the 200-bit version. The proposed work is compared to 256-bit, 192-bit, and 128-bit AES systems in terms of encryption and decryption times and throughput on both sides.

Efficient Data Hiding Using AES & Advanced Hill Cipher Algorithm

This paper proposes a data hiding technique using the AES algorithm, combining steganography and cryptography for enhanced security. While cryptography alone cannot provide absolute security, combining it with steganography results in an advanced security solution. Among various cryptography techniques, AES encryption with a 128-bit key is employed to conceal the message. The proposed hybrid scheme, which incorporates the advanced Hill cipher algorithm and AES, enhances security, as indicated by several metrics.

V. RESULTS

In this comprehensive review paper on Network Security and Cryptography, we have examined a wide range of topics and findings relevant to the field. The following key results and conclusions have emerged from our analysis:

Evolution of Threat Landscape: Our review underscores the dynamic and evolving nature of the threat landscape in network security. Cyberattacks have become increasingly sophisticated, emphasizing the need for continuous innovation in security measures.

Importance of Encryption: Cryptography remains a cornerstone of network security. The importance of encryption techniques, both symmetric and asymmetric, cannot be overstated in safeguarding data during transmission and storage.

Key Management: Effective key management is crucial for secure data exchange. Secure key generation, distribution, and storage mechanisms are essential components of a robust security infrastructure.

VI. CONCLUSION

In today's rapidly evolving digital landscape, network and data security have become essential concerns for any organization with an internal private network connected to the internet. The protection of data has become critically important, particularly when it comes to ensuring user data security in cloud environments. With the advancement of cryptographic techniques and the increasing use of multiple keys for a single application, the field of cryptography has become more flexible and adaptable. This paper has introduced various cryptographic schemes used for network security purposes. The encryption of messages with highly secure keys, known only to the sender and recipient, plays a significant role in achieving robust security in the cloud. The secure exchange of keys between the sender and receiver is a crucial task, and key management is vital for maintaining the confidentiality of sensitive information and verifying the integrity of exchanged messages to ensure authenticity. Network security encompasses the application of cryptographic algorithms in network protocols and applications. This paper has provided a brief overview of computer security concepts and highlighted the future challenges in computer network security. Future work in this field should focus on key distribution and management, as well as selecting the most suitable cryptographic algorithms to enhance data security in cloud environments.

VII. REFERENCES

[1] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[2] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[3] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[4] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.

[5] Ritu Pahal, Vikas Kumar, “Efficient implementation of AES”, International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[6] N.Lalitha, P.Manimegalai, V.P. Muthu kumar, M. Santha, “Efficient data hiding by using AES and advance Hill cipher algorithm”, International journal of research in computer applications and Robotics, volume 2, issue 1, January 2014.