Review on Network Security and Cryptography

Mr. Pradeep Nayak[1], Shrinidhi M H[2], Siddharth N[3], Shraddha[4] ,Shreya Rao[5]

Department of Computer Science and Engineering (IOT)[1-5]

Alva's Institute of Engineering and Technology, Mijar, Karnataka, India
pradeep@aiet.org.in,hegdes300@gmail.com,siddharthkadwad@gmail.com,
shraddhapoojary815@gmail.com, raoshreya477@gmail.com

Abstract

The rapid advancement of internet and information technologies, alongside the proliferation of e-commerce platforms and social networks, has significantly increased global connectivity. This connectivity has led to the generation of vast volumes of data while simultaneously exposing networks to a growing array of cyber threats. Malicious actors leverage tactics such as phishing, Trojan horses, and backdoor viruses to exploit vulnerabilities, paralyze systems, and target high-value entities such as military and government networks, posing significant threats to national and social security[1]. Network security is essential in mitigating these risks, encompassing mechanisms such as access control, firewalls, endpoint security, and antivirus programs. Cryptography, a cornerstone of network security, ensures the confidentiality, integrity, and authenticity of information by encoding data into secure formats using mathematical algorithms. Processes like encryption and decryption protect data from unauthorized access, making cryptography critical for safeguarding sensitive communications. Despite its efficacy, cryptography faces challenges, particularly in resource-constrained environments such as sensor networks and cloud storage. Secure key exchange remains a complex task, and ensuring data confidentiality in cloud storage systems demands robust encryption mechanisms that prevent unauthorized access while allowing secure search capabilities. This paper provides a comprehensive review of network security and cryptographic methodologies, highlighting their applications, challenges, and advancements. It explores how these techniques address evolving cyber threats, offering insights into the critical role of cryptography in modern information security.[2]

Keywords:- *Cryptography, network security, encryption, data confidentiality, cyber-attacks, cloud storage, sensor networks*

1. INTRODUCTION

The rapid advancement of modern internet and information technologies has transformed the way individuals, enterprises, educational institutions, and government entities connect and operate. This increased connectivity has significantly enhanced communication, data sharing, and efficiency but has also exposed systems to a growing array of cyber threats. Malicious actors exploit vulnerabilities through fake websites, phishing emails, Trojan horses, and backdoor viruses to attack and disrupt networks. The primary targets of these attacks are computers, and once infiltrated, entire networks can be rendered inoperative. Military and government entities are particularly high-value targets, with breaches posing severe threats to national and social security.

Network security plays a vital role in safeguarding data from these threats. It encompasses various mechanisms, including access control, firewalls, endpoint security, antivirus programs, and encryption. Cryptography, often referred to as the science of "Hidden Secrets," is a cornerstone of network security. It employs mathematical algorithms to encode information, ensuring its confidentiality, integrity, and authenticity. Cryptographic processes such as encryption and decryption transform plaintext into ciphertext and vice versa, protecting data from unauthorized access and tampering.

Despite its effectiveness, cryptography faces challenges, particularly in resource-constrained environments like sensor networks and remote cloud storage. Key management, the secure exchange of encryption keys between

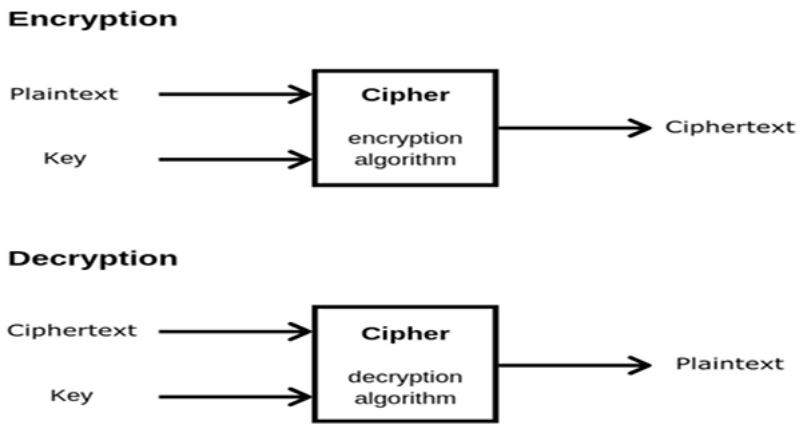

Fig.1. Plaintext & ciphertext

sender and recipient is a critical yet complex task in sensor networks. Similarly, in cloud storage, data must be encrypted by users before outsourcing, ensuring that even service providers cannot decipher the data. Moreover, cloud systems must enable secure search capabilities, allowing users to access specific encrypted segments without exposing their content.

This paper reviews the foundational principles of network security and cryptography, examines current methodologies, and explores their applications in addressing evolving cyber threats. By highlighting the strengths and limitations of existing approaches, this work aims to provide insights into the ongoing advancements in secure communication and data protection.

2. TYPES OF SECURITY ATTACKS

The Internet of Things (IoT) encompasses a wide range of applications, from automating homes and offices to monitoring production lines and tracking products in retail environments. The potential for applications is vast and continually expanding. A dedicated IoT service can be utilized for each specific application to enhance development efficiency and accelerate the implementation process. The following categorizations are adapted from [3].

2.1. PASSIVE ATTACKS

This type of attack includes observation or monitoring of communication. A passive attack attempts to learn or make use of information from the system but does not affect system resources. The goal of the opponent is to obtain information that is being transmitted. Types of passive attacks:

• Traffic Analysis: The message traffic is sent and received in a normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.

• Release of Message Contents: Read the message's contents from sender to receiver.

2.2. ACTIVE ATTACKS

An active attack attempts to alter system resources or affect their operation. It involves some modification of the data stream or the creation of a false stream. Types of active attacks:

• Modification of Messages: some portion of a legitimate message is altered, or messages are delayed or reordered.

• Denial of Service: An entity may suppress all messages directed to a particular destination.

• Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

• Masquerade: It takes place when one entity pretends to be a different entity. [4]

3. SECURITY SERVICES

A service provided by the protocol layer of open systems, ensuring the security of both system operations and data transfers. It enhances the security of data processing and transfer.

3.1. DATA INTEGRITY

It can be applied to a stream of messages, a single message, or specific fields within a message. Integrity loss refers to unauthorized modifications or destruction of information. It ensures that the information remains unaltered and is not tampered with during transmission or storage. Integrity mechanisms such as checksums or hashes are commonly used to detect any unauthorized modifications.

3.2.DATA CONFIDENTIALITY

Maintaining authorized restrictions on access to and disclosure of information, including measures to protect personal privacy and proprietary data. Confidentiality loss occurs when information is disclosed without authorization, potentially leading to unauthorized access and potential misuse of sensitive information.

3.3. AUTHENTICITY

Authentication ensures that only authorized nodes can participate in communication, preventing unauthorized access and maintaining data integrity[5]. Additionally, it plays a crucial role in optimizing the efficient use of limited resources, minimizing the risk of resource exhaustion, and preventing unauthorized consumption, ensuring the smooth and secure operation of the network.

3.4. NONREPUDIATION

Nonrepudiation ensures that neither the sender nor the receiver can deny having transmitted or received a message. This means that once a message is sent, the receiver can prove the sender's identity, and once a message is received, the sender can verify the recipient's identity.

3.5. ACCESS CONTROL

Access control involves the ability to restrict and manage access to host systems and applications through communication links. To accomplish this, each entity seeking access must first be identified or authenticated, ensuring that access rights are granted based on individual permissions. This helps prevent unauthorized access and protects sensitive information from being accessed by unauthorized parties. Effective access control mechanisms are essential for maintaining the confidentiality, integrity, and availability of systems and data.

4. NETWORK SECURITY MODEL

Figure 1 illustrates the network security model, where a message is transferred from one party to another across an Internet service. A third party may be responsible for distributing the secret information to both the sender and receiver while ensuring it remains hidden from any adversary [6]. Security measures come into play when it is necessary to protect information from potential threats such as confidentiality, authenticity, and more. All security techniques consist of two key components: A security-related transformation is applied to the information being transmitted, ensuring the message is encrypted using a key, making it unreadable to unauthorized parties. An encryption key that, in combination with the transformation, scrambles the message before transmission and unscrambles it upon reception.

Additionally, secure key management ensures that only authorized parties have access to the encryption keys, reducing the risk of unauthorized access to sensitive data. Efficient key management systems must address aspects such as secure key storage, controlled access to key stores, and backup mechanisms to ensure the keys are not lost or compromised. These key management practices are crucial to maintaining data confidentiality and integrity, particularly in cloud environments where data is often distributed and accessed across multiple systems.

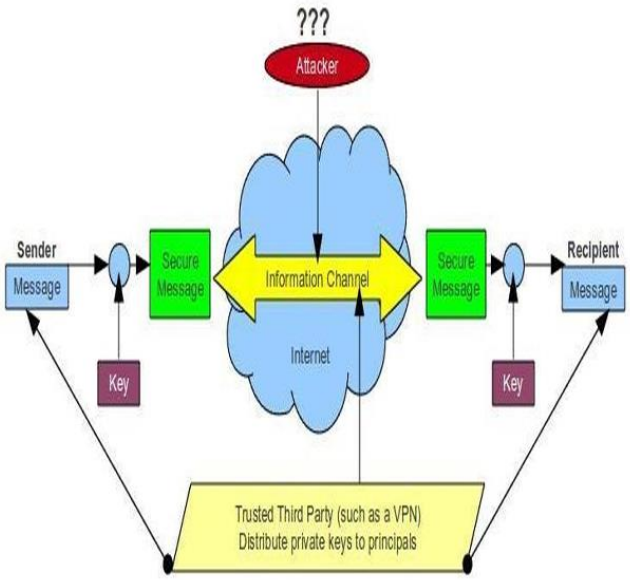

Figure 1. Model for Network Security

4.1. NEED FOR KEY MANAGEMENT IN THE CLOUD

The need for key management in the cloud arises because encryption provides data protection, while key management ensures access to that protected data. It is strongly recommended to encrypt data both in transit over networks, at rest, and on backup media. Specifically, data owners must manage their encryption keys. Both encryption and key management are crucial for securing applications and data stored in the cloud. Below, we discuss key requirements for effective key management:

Secure Key Stores: Key stores must be protected from unauthorized access. 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 secured during storage, transit, and backup media.[7]

Access to Key Stores: Access to key stores should be limited to users with the appropriate permissions. Role separation is essential to control access, ensuring that the entity using a key is not the same entity that stores it.

Key Backup and Recoverability: Keys require secure backup and recovery solutions. The loss of keys can effectively deny access to encrypted data, posing a significant risk to businesses. Cloud providers must ensure that keys are not lost and have reliable backup and recovery mechanisms in place.

5. CRYPTOGRAPHY MECHANISM

Cryptography is a method used to store and transmit data in a format that can only be read and processed by intended recipients. The concept is primarily associated with transforming plaintext messages (ordinary text, also referred to as cleartext) into ciphertext through a process known as encryption and converting it back through decryption. Generally, there are three main types of cryptographic schemes used to achieve these objectives: secret key (symmetric) cryptography, public key (asymmetric) cryptography, and hash functions, each of which is explained below.

5.1. SECRET KEY CRYPTOGRAPHY

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 2, the sender A uses the key K (or some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies the same key K (or ruleset) to decrypt the ciphertext C and recover the plaintext message M. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

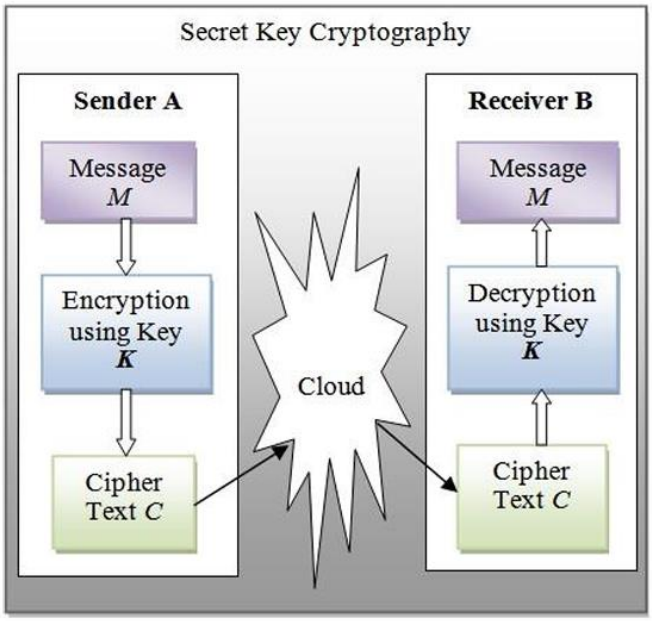

Figure 2. Secret Key Cryptography

With this form of cryptography, the key must be securely exchanged and known to both the sender and the receiver, particularly in computer networks. The biggest difficulty with this approach, of course, is the distribution of the key. Secure key exchange and management are crucial in network environments to ensure that unauthorized parties cannot gain access to the encryption keys. Without proper key management, there is a risk of unauthorized access to sensitive data, making network security more vulnerable to attacks such as brute-force attacks, especially when using the ECB mode.

Secret key cryptography schemes are generally categorized as stream or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism to constantly change the key. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher, whereas the same plaintext will encrypt to different ciphertexts in a stream cipher.

Electronic Codebook (ECB) mode: The simplest, most obvious application, where the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks will always generate the same ciphertext block, which is susceptible to various brute-force attacks.

Cipher Block Chaining (CBC) mode: Adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is XORed with the previous ciphertext block before encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext. This makes CBC more secure for network environments.[8]

Cipher Feedback (CFB) mode: A block cipher implementation that operates as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input over networks.

Output Feedback (OFB) mode: A block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

5.2. PUBLIC-KEY CRYPTOGRAPHY

Public-key cryptography, also known as asymmetric cryptography, is a fundamental component of modern computer network security. It involves the use of two distinct keys: a public key and a private key. The public key is made available to everyone, allowing any sender to encrypt data securely, while the private key remains confidential and is used by the recipient to decrypt the message. This asymmetry ensures that even if an attacker

intercepts the public key, they cannot derive the corresponding private key, providing strong security guarantees. In computer networks, public-key cryptography is essential for various applications, including secure communication, authentication, and key exchange.

In network security, public-key cryptography plays a crucial role in securing protocols such as Transport Layer Security (TLS), which ensures secure communication between clients and servers. For instance, during an HTTPS session, a server provides its public key to a client, allowing the client to encrypt the session data. The server then decrypts this data using its private key, ensuring the confidentiality and integrity of the communication. Similarly, public-key cryptography is vital for securing Virtual Private Networks (VPNs), where public-key infrastructure (PKI) is used to manage certificates, authenticate users, and establish encrypted tunnels between remote devices.

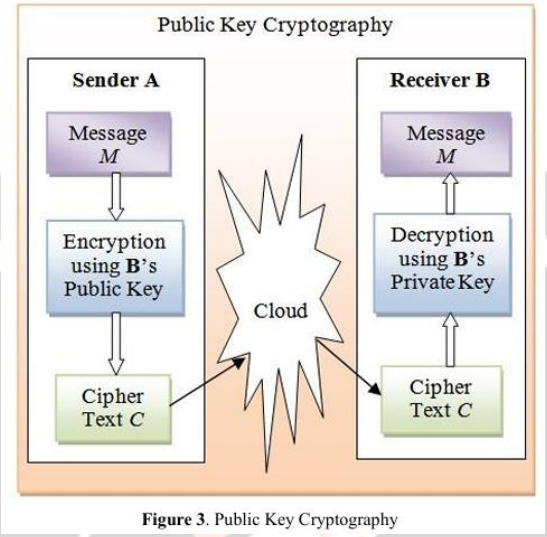

Figure 3. Public Key Cryptography

Public-key cryptography also enhances data integrity and authentication. Digital signatures, generated using a sender's private key, ensure that the data was not tampered with during transmission and authenticate the sender. The recipient can verify these signatures using the sender's public key, ensuring non-repudiation. This feature is particularly important in secure email systems and digital certificates, which are used in various network applications like secure email protocols (e.g., S/MIME) and Secure Sockets Layer (SSL) certificates.[9]

In conclusion, public-key cryptography is a cornerstone of network security, offering solutions for secure communication, authentication, key exchange, and integrity verification. Its application across various computer network concepts, such as TLS, VPNs, PKI, and secure email, underscores its significance in safeguarding data and maintaining robust security in modern networks.

5.2.1.RSA

RSA, named after the three MIT mathematicians who developed it—Ronald Rivest, Adi Shamir, and Leonard Adleman [14]—is one of the most widely used public-key cryptography implementations. In computer networks, RSA is applied in numerous software products for key exchange, digital signatures, and encryption of small blocks of data. The RSA algorithm utilizes a variable-size encryption block and key, with the key-pair derived from two large prime numbers, each potentially consisting of 100 or more digits. These prime numbers are chosen following specific rules, resulting in an n value that is roughly twice as long as the prime factors. In the context of computer networks, RSA plays a critical role in securing data transmitted over communication channels such as HTTPS, ensuring secure web communication. RSA operates through three main phases: Key Generation, Encryption, and Decryption.

5.2.1.1. Key Generation Phase

The receiver generates a public/private key pair. The algorithm is as follows:

1) Select p, q such that p and q both are prime, $p \neq q$

2) Calculate n = p * q

3) Calculate f(n) = (p - 1)(q - 1)

4) Select integer e such that gcd(f(n), e) = 1; 1 < e < f(n)

5) Calculate d such that d≡ e-1 (mod f(n))

6) Public key PUK= (e, n)

7) Private key PRK=(d, n)

5.2.1.2. Encryption Phase

Encryption is done by the sender with the receiver's Public Key.

The algorithm is as follows:

1) Plain Text M is known, M < n

2) Cipher Text C is calculated as

$C = M^e \bmod n$

5.2.1.3. Decryption Phase

Decryption is done by the receiver using his Private Key. The algorithm is as follows:

1) Cipher Text C is known

2) Plain Text M is calculated as

$M = C^d \bmod n$

5.2.2. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is an advanced public key cryptographic algorithm that is widely utilized in computer networks due to its efficiency and strong security properties. ECC [16,17] is based on elliptic curve arithmetic, which operates over finite fields.[17]

In computer networks, ECC is particularly useful for key exchange protocols such as the Elliptic Curve Diffie-Hellman (ECDH) algorithm. ECDH enables secure key establishment between parties over insecure channels, ensuring that only authorized entities can generate shared secrets. This is especially important in environments with limited bandwidth and processing capabilities, such as mobile and IoT networks, where traditional public key cryptography may impose excessive computational overhead. Furthermore, ECC's ability to generate smaller key sizes while maintaining high-security levels makes it ideal for environments where resource constraints are a concern. In computer networks, ECC plays a vital role in protecting sensitive data in cloud computing, secure messaging, and other applications where robust, yet efficient encryption is essential for maintaining data integrity and confidentiality.

6. COMPUTER NETWORK AND INTERNET SECURITY

Internet security is a branch of computer security specifically focused on protecting data and systems connected to the Internet. It involves securing web browsers and other network-connected applications or operating systems. The primary goal is to establish rules and protective measures to defend against various online threats such as intrusion, fraud, and phishing attacks. Due to the inherent insecurity of Internet channels for data exchange, ensuring data confidentiality and integrity becomes essential, often achieved through encryption. Network security refers to the process of controlling and authorizing access to data within a network environment.

Network administrators manage this by assigning IDs, passwords, or other forms of authentication to ensure that users can access information and programs only within their permitted scope of authority. This helps protect

sensitive information from unauthorized access and maintains the integrity and confidentiality of network data.

Types of Network Security:

6.1. WIRELESS NETWORK SECURITY

Wireless network security protects computers and data transmitted via wireless networks from unauthorized access and potential threats. The most commonly used wireless security protocols are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is widely regarded as a weak security standard, as its password can often be cracked using basic tools and a laptop in just a few minutes. WPA, on the other hand, is secured primarily through Wireless Transport Layer Security (WTLS), which ensures secure communication between mobile devices (clients) and the WAP gateway connecting to the Internet.

There are several approaches to achieving end-to-end WAP security. One approach assumes that the mobile device implements TLS over TCP/IP, and the wireless network supports the transfer of IP packets. The WAP architecture addresses two key challenges of wireless web access: the limitations of mobile devices such as small screen size and limited input capabilities, as well as the low data rates of wireless networks. Two key WTLS concepts are the secure connection and the secure session:[16]

Secure connection refers to a transport layer connection that provides suitable service, typically between peers in an SSL context, and is transient. Multiple secure connections may exist between parties, but only one session is usually active at a time.

Secure session refers to an association between a client and a server, established through the Handshake Protocol, defining cryptographic security parameters that can be shared across multiple connections to avoid repeated security negotiations. These concepts are fundamental to maintaining secure communication over wireless networks.

6.2. IP SECURITY

Internet Protocol Security (IPsec) is a protocol suite designed to secure Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a session. IPsec includes protocols that enable mutual authentication between agents at the beginning of a session and the negotiation of cryptographic keys used throughout the session. It can be employed to protect data flows between two hosts (host-to-host), between two security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec is particularly useful for implementing virtual private networks (VPNs) and enabling remote user access through dial-up connections to private networks. A significant advantage of IPsec is that security configurations can be applied without requiring changes to individual user computers.[11]

IPsec offers two primary security services: the Authentication Header (AH), which provides sender authentication, and the Encapsulating Security Payload (ESP), which supports both sender authentication and data encryption. The information for these services is inserted into the packet within a header that follows the IP packet header. Key management protocols, such as ISAKMP/Oakley, are used to establish secure key exchanges. IPsec employs cryptographic security services to protect communications over IP networks, supporting network-level peer authentication, data origin authentication, data integrity, confidentiality through encryption, and replay protection. It secures application traffic over any IP network, allowing applications to be automatically secured at the IP layer.

6.3. ELECTRONIC MAIL SECURITY

Email is susceptible to both passive and active attacks, making its protection from unauthorized access and inspection essential, a concept known as electronic privacy[12]. In countries with constitutional guarantees of the secrecy of correspondence, email is treated similarly to letters and legally protected from eavesdropping. With the increasing reliance on email, there is a growing demand for authentication and confidentiality services. Two prominent schemes widely used for email security are Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extension (S/MIME).

PGP is an open-source, freely available software package that provides email security through authentication using digital signatures, confidentiality via symmetric block encryption, compression through the ZIP algorithm, and email compatibility through radix-64 encoding. PGP incorporates tools for public-key trust models and public-key certificate management. S/MIME, on the other hand, is an internet-standard approach to email security, offering the same functionality as PGP. It serves as a security enhancement to the MIME internet email format and is based on technology developed by RSA Data Security.

6.3.4. TRANSPORT LEVEL SECURITY

Transport Layer Security (TLS) is an IETF standardization effort aimed at producing an internet-standard version of SSL. Secure Socket Layer (SSL) provides security services between TCP and the applications that use TCP. The internet-standard version is called TLS. The TLS Record Format is identical to the SSL Record Format. SSL/TLS offers confidentiality using symmetric encryption and ensures message integrity through a message authentication code. SSL/TLS also includes protocol mechanisms that enable two TCP users to negotiate the security mechanisms and services they will use. HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to ensure secure communication between a web browser and a web server.[13]

Secure Shell (SSH) provides secure remote login and other secure client/server facilities. The SSH Connection Protocol operates on top of the SSH Transport Layer Protocol and assumes a secure authenticated connection is in use. All types of communication via SSH, such as terminal sessions, are supported using separate channels.

7. CONCLUSION

The exponential growth of internet technologies and digital connectivity has transformed the global landscape, making network security and cryptography paramount concerns for organizations worldwide. As digital infrastructures become increasingly complex and interconnected, the potential for cyber threats has escalated dramatically, necessitating robust and sophisticated security mechanisms. Cryptographic techniques have emerged as critical tools in protecting sensitive data, with advanced mathematical algorithms enabling more versatile and multi-layered encryption strategies[14]. The landscape of network security is characterized by continuous evolution, where traditional security approaches are constantly challenged by emerging threats. From passive attacks like traffic analysis to active attacks involving message modification and masquerading, the spectrum of potential security breaches has grown increasingly sophisticated. Cryptographic methods, including symmetric and asymmetric encryption, provide essential defense mechanisms by ensuring data confidentiality, integrity, and authenticity through complex mathematical transformations and secure key management protocols.

Key management has become a central challenge in maintaining network security, particularly in resource-constrained environments like cloud storage and sensor networks. The secure exchange of encryption keys between sender and receiver represents a critical task that directly impacts the overall effectiveness of cryptographic systems. As organizations increasingly rely on cloud infrastructures and distributed computing environments, developing more efficient and robust key distribution mechanisms becomes imperative for protecting sensitive information from unauthorized access.[15]

Looking forward, the future of network security and cryptography lies in continuous innovation and adaptation. Researchers and cybersecurity professionals must focus on developing more sophisticated algorithms, improving key distribution techniques, and creating adaptive security frameworks that can respond dynamically to emerging threats. The ultimate goal remains to create comprehensive security ecosystems that can protect digital assets while maintaining the flexibility and efficiency required in modern computational environments.

This ongoing journey of enhancing network security underscores the critical intersection of mathematics, computer science, and cybersecurity. As digital technologies continue to advance, the development of more intelligent, versatile, and resilient cryptographic methods will be essential in safeguarding the integrity of global information systems and protecting the privacy of individuals and organizations alike.

REFERENCES

[1] 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

[2] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.

[3] Bellare, September Mihir; Rogaway, Phillip (21 2005). "Introduction". Introduction to Modern Cryptography. p. 10.

[4] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. “A. Handbook of Applied Cryptography”. ISBN 0-8493-8523-7.

[5] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

[6] S. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004.

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

[8] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 26, 2001.

[9] Bruce Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings (Springer-Verlag): 191 204.

[10] Schneier, Bruce (2005-11-23). "Twofish Cryptanalysis Rumors". Schneier on Security blog. Retrieved 2013-01-14.

[11] Matsui, Mitsuru; Tokita, Toshio (Dec 2000). "MISTY, KASUMI and Camellia Cipher Algorithm Development". Mitsibishi Electric Advance (Mitsibishi Electric corp.) 100: 2-8. ISSN 1345-3041.

[12] General Report on the Design, Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms". 3GPP. 2009

[13] O. Dunkelman, N. Keller, A. Shamir, \A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony," Advances in Cryptology, Proceedings Crypto'10, LNCS, T. Rabin, Ed., Springer, Heidelberg, 2010

[14] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[15] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644-654.

[16] Koblitz, N., 1987. “Elliptic curve cryptosystems. Mathematics of Computation” 48, 203-209.

[17] Miller, V., 1985. “Use of elliptic curves in cryptography”. CRYPTO 85.