International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 07 | July 2024 www.irjet.net p-ISSN: 2395-0072

Protecting Digital Information: A Review of Network Security and Cryptography

Shreejith Kinnal[1], Shreya E[2], Aditi Parvati[3], Satwika S[4], Prajwal Angadi[5]

Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Karnataka, India

---

Abstract - *In today's technology-centered society, network security is crucial because of the growing reliance on digital systems and the potential consequences of security breaches. To protect sensitive information and guarantee the continuous operation of numerous companies and sectors, computer networks must be protected. Employing robust security mechanisms, including intrusion detection systems, firewalls, and encryption is essential to preventing unauthorized access and data tampering. Emerging dangers, including malware, eavesdropping, and social engineering, however, present serious risks. Organizations may reduce risks, secure their network infrastructure and data, and ensure data confidentiality and integrity by putting in place robust security measures and staying attentive.*

***Key Words*: Network, cryptography, security, encryption, decryption, key, ssl.**

1.INTRODUCTION

Due to the growing reliance on digital systems and the potential repercussions of security breaches, network security is of the utmost importance. To protect computer networks is essential for securing private data and maintaining the proper operation of many different companies and sectors in today's technology-driven world. Implementing strong defenses against firewalls, encryption, access controls, and intrusion detection systems(IDS). Together, these security measures protect data's confidentiality, integrity, and availability and create secure communication channels. On the other hand, as technology develops, new dangers keep popping up. There are several serious risks that organizations and individuals must be aware of, including malware, phishing attempts, network eavesdropping, and social engineering attacks. It is possible that these malevolent actions will result in financial losses, reputational damage, and privacy violations.

2. NETWORK SECURITY

With the exponential growth of the internet and the widespread adoption of information-centric applications, ensuring the security of data transmitted, stored, and sent through the network has become paramount. Unauthorized access to this data poses a significant threat, as hackers employ various malicious techniques, including the deployment of viruses, to compromise network integrity. To mitigate these risks, robust network security systems are implemented to thwart potential attacks and respond swiftly in the event of a data breach. The field of computer network security encompasses various fields of study, incorporating ideas and concepts from computer technology, communication technology, mathematics, cryptography, information theory, management, and law. It demands an integration of diverse solutions from these fields to effectively address the intricate challenges associated with network security.

3. NETWORK SECURITY OBJECTIVES

i. Confidentiality: Network security measures are implemented to ensure that information is accessible only to authorized users, safeguarding it from unauthorized access or disclosure.

ii. Authenticity: The system guarantees the receiver that the information received is indeed from the claimed source, verifying its

authenticity and preventing spoofing or impersonation.

iii. Integrity: Network security ensures that only authorized users have the ability to modify or alter information, maintaining its integrity and preventing unauthorized tampering or manipulation.

iv. Dependability: Network security measures prevent both senders and receivers from denying the transmission or receipt of messages, establishing a reliable and trustworthy communication environment.

v. Availability: Authorized users should have uninterrupted access to the required information resources and services, ensuring the availability of network resources without compromising security.

vi. Auditability: The system incorporates mechanisms that allow for the review and monitoring of all security-related activities within the network, enabling the identification and investigation of potential security breaches or anomalies.

4. NETWORK SECURITY THREAT

Network security threats is nothing but the potential risks and vulnerabilities of the network which can compromise

the security. Nowadays threat detection and management is just as important any other field in computer networking. Just as in real life, threats can come in different types; in computer networks too, threats can be of various types. Some of the most common threats to network security are

4.1. Spoofing of Network Traffic

Spoofing is a common technique hackers use to access the data packets while in transition from the source to destination. The message transmitted over the network contains vital information such as the source and destination IP address. The intruder initially finds out the IP address of the trusted host and modifies the header content in such a way that the message appears to be coming from the trusted source, but in reality, it is from the attacker.

4.2. Unauthorized modification

Unauthorized modification of data poses a significant threat to data integrity, potentially resulting in severe consequences such as database or spreadsheet corruption and disruption of critical applications. Even minor unauthorized changes to software can lead to the compromise of the entire operating system and associated applications, necessitating reinstallation efforts. These modifications can be initiated by both unauthorized individuals and authorized users. Data or application alterations have the potential to redirect information to unintended destinations, enabling external actors or hackers to manipulate and forward the modified data. Several factors contribute to the occurrence of unauthorized modifications, including:

i. Insufficient data encryption measures.

ii. Inappropriate assignment of write permissions to users who only require read access.

iii. Inadequate protection tools.

5. NETWORK SECURITY TECHNOLOGIES

Technologies mainly applied in network security are authentication, data encryption technology, firewall technology, intrusion detection system (IDS), antivirus technology, virtual private network (VPN) and other technologies, in which authentication and encryption, firewall and IDS are the most important defensive lines of network security

5.1. Firewall

Firewalls are one of the most important and widely used software, hardware tools used for the purpose of network security. The main objective of a firewall is to prevent intrusion by outsiders thus keeping the data of the user safe from unauthorized users or hackers [15]. Firewalls control as well as monitor incoming and outgoing traffic on a network using predefined set of rules. The fundamental technology behind a firewall system can be classified as follows:

5.1.1 Packet-Filter Firewall

Packet filtering is one of the earliest firewall technologies deployed. A packet filter can either forward or block packets based on the information in the network layer and transport layer headers, out of which the IP addresses, source and destination port addresses and type of protocol such as TCP and UDP are closely monitored

According to the figure, the following packets are filtered

Table -1: Packet Filter Firewall Ruleset

Interface	Source IP	Source Port	Destination IP	Destination Port
1	172.58.0.0	Any	Any	Any
1	Any	Any	Any	23
1	Any	Any	192.47.20.8	Any
2	Any	Any	Any	80

i. Incoming packets from network 172.58.0.0 are blocked for security reasons.

ii. Incoming packets destined for any internal TELNET server (port 23) are blocked.

iii. Incoming packets destined for internal host 192.47.20.8 are blocked.

iv. Outgoing packets destined for HTTP server port 80 are block

5.1.2 Proxy firewall

The major drawback of packet-filter firewall is that it is restricted to network and transport layers. This poses a major inconvenience and threat whenever the user wants to filter a message based on the information available in the message itself. This can be one only using proxy firewalls which extends its service till the application layer. Following are the several applications that can support proxy firewalls: -

i. HTTP (Web)

ii. HTTPS/SSL (Secure Web)

iii. SMTP (email)

iv. POP3 (email)

v. IMAP (email)

vi. NNTP (newsreaders)

vii. Telnet (Shell access)

Proxy firewalls, while effective in securing network communications, have a few notable disadvantages that should be considered. One drawback is the increased latency they introduce. Proxy firewalls involve additional steps in the processing and inspection of network traffic. This can cause a delay in the delivery of data packets, which can negatively impact real-time applications or time-sensitive communication. In high-demand scenarios, the processing burden on the firewall may exceed its capacity, resulting in performance degradation or network slowdowns. This limitation should be carefully evaluated to ensure that the chosen proxy firewall can handle the expected volume of network traffic without compromising system performance.

However due to the increasing network security threats and increased traffic on the internet day by day, traditional firewalls merely are proven to be ineffective, hence the need of New Generation Firewall (NGFW) technologies are being established, which incorporates Intrusion Detection and Prevention (IDP) features to enhance security.

6.NETWORK SECURITY PROTOCOLS

Secure Socket Layer

The Secure Socket Layer (SSL) is one of the most important protocols used to establish a secure communication channel from the server to client or simply from a source to the respective destination. The SSL is implemented in between the application layer and the transport layer [14]. The protocols used in SSL are:

The SSL handshake protocol is the first step in establishing a secure communication by identifying the client and server. The handshake protocol also decides on information regarding the cryptographic algorithm used, public key encryption techniques and protocol version.

The SSL Change Cipher Protocol is used to notify both the client and server that the packets that are about to be sent will be encrypted using the algorithm decided in the upper layers.

The SSL Alert Protocol, as the name suggests allows both client and server to send an alert message in-case of any suspicious activity

The SSL Record Protocol takes messages from higher-level protocols (like Handshake, ChangeCipherSpec, Alert, or the application layer). It divides the message into smaller pieces if needed and may compress it. Then, a cryptographic checksum called a MAC(Message Authentication Code) is added to the compressed message using the agreed-upon hash algorithm. The compressed fragment along with the MAC is encrypted using the agreed-upon encryption algorithm. Lastly, the SSL header is attached to the encrypted message.

7.INTRODUCTION TO CRYPTOGRAPHY

Since the world has become more digitally connected, all work and activities are carried out online. The Majority of the work which was operating in offline mode has shifted to online mode. Though it is more reliable and easier along with it comes the question of privacy and security [10]. With the connection of the internet, the world generates a huge amount of data every minute. All the information or data are prone to be attracted by cyber-attacks [5]. This can be prevented by the artwork called cryptography. Cryptography is an abstract concept derived from Greek, in which "CRYPTO" refers to secrets and "GRAPHY" to writing. Cryptography is a technique where only the sender and the receiver can understand the information communicated between them. Cryptography has been in use in many forms since the 2000B.C. Cryptography roots are found in Roman and Egyptian civilization. As days passed by, the way of using cryptography evolved. Billions of people are totally unaware that they are using cryptography on a daily basis.

8.CRYPTOGRAPHY MECHANISM

Cryptography has a specific mechanism that it follows. Information that needs to be conveyed is referred to as plain text. In this case, it is the original text that the sender wishes to protect from possible cyber attacks. These plain texts can be pictures, characters, documents. The process of disguising the plain text [6] is called as encryption. It is done to prevent the unauthorized access of the information. This data encryption is done with algorithms.

The information which is known as a cipher text. It is basically the text which is unreadable or encode information of the message. It is a gibberish text [10]. It is meaningless data. Well this encryption is dependent on the key which is called an encryption key. Key is the input to the encryption algorithm. Keys are defined as numbers or characters, that are used to encode plain text into cipher text [10]. Both the sender and receiver will have access to this key. Each key used for these algorithms will be unique and unpredictable [10]. In contrast to encryption, decryption involves the conversion of an encrypted or coded message into plain text or back to the original message. This process is carried out by the receiving side. For decryption, the receiver needs the secret key.

9.CHARACTERISTICS OF CRYPTOGRAPHY

Confidentiality: It is one of the most important characteristics of cryptography. It protects the data and

prevents the data from being accessed by the unauthorized entity. Only the person having the key can access the information. It verifies the message source.

Authentication: It is the process of making sure of the identities of the sender and receiver. By this it makes sure that the information is communicated between the claimed sender and the receiver.

Data integrity: It ensures that the information or data hasn't been modified or altered after the sender sends it[2]. Basically, it ensures that the information is uncorrupted intentionally or accidentally. Data integrity can be achieved by the method of using hashing at the sender and the receiver end.

Non-repudiation: By using this process, the sender and intended recipient can be ensured that the message was sent by the true sender and received by the intended recipient and not by an unauthorized recipient. By this mechanism neither the sender nor the receiver can be able to put the false accusation about not receiving the message [11] .

10.TYPES OF ENCRYPTION

Cryptography can be classified into two main types, symmetric encryption and asymmetric encryption.

10.1. Symmetric encryption

In addition to symmetric encryption, secret key cryptography and private key cryptography are also the terms used to describe symmetric encryption. This is one of the most widely known and oldest techniques of cryptography [1].For encrypting the data the sender uses a secret key. A secret key can be a word or a number. There is a shared secret key between the sender and receiver. Both encryption and decryption of the message are accomplished with this one key. For this reason it is known as symmetric encryption.

Pros of symmetric encryption:-

i. It is efficient to compute a large amount of data. [10]

ii. It is fast compared to asymmetric encryption

iii. It has low computing power

Cons of symmetric encryption:- As only one secret key is used to encrypt and decrypt the message, they must transport their secret keys safely [5].

10.2. Asymmetric encryption

In addition to asymmetric encryption, public key encryption is also known as key exchange encryption. This encryption technique allows us to use different keys for both encrypting and decrypting [6]. In general, there are two key types: a public key and a private key [6]. Everyone has access to the public key. Anyone can use a public key to transmit an encrypted message. Only the recipient's private key can decrypt this encrypted message. These two keys will be associated mathematically [5].

AES

AES stands for the “Advanced encryption standard”. NIST introduced this algorithm in 2001 [10]. It is one of the most powerful algorithms. AES is a symmetric block cipher encryption algorithm. AES supports 128 bits of data of any combination. A key may have a length of 128,192, or 256 bits. Rounds are determined by the length of the key.

i. 10 rounds for 128 bit keys.

ii. 12 rounds for 192 bit keys.

iii. 14 rounds for 256 bit keys .[3]

128 bits(16 bytes) are represented in the form of 4 x 4 matrix [9].

Each round consists of 4 sub-process

- Substitute byte transformation:- By looking up a fixed table provided in the design, each byte is replaced by another byte. This method produces a 4 x 4 matrix. [3].
- Shift row transformation:- All bytes except the first row of the matrix are shifted in a cyclic order to the left. There is a shift of 1 byte to the left in the second row. There is a shift of 2 bytes to the left in the third row. There is a shift of 3 bytes to the left in the fourth row. [3]. The result of this method is the shifted position of the 16 bytes.
- Mixcolumns transformation:- In this step we perform multiplication. A fix matrix is multiplied to each column vector [8]
- AddRoundKey transformation:- It is the most important step in the AES algorithm. A 4 x 4 matrix of bytes is used to store the input data and key. A round key consisting of 128 bits is XORed with the 128 bits in the matrix. By doing this, it gives the cipher text which is the output of this step.

DES

DES stands for “Data encryption standards”. DES is one kind of symmetric block cipher. In 1974, IBM and the US government jointly developed this algorithm [8]. A 56-bit secret key is required for DES to support or encrypt data in a 64-bit block. In this method, there are 16 rounds to encrypt the data [1]. Initially, the key length was 64 bits, but it was later decided that 56 bits would be used to encrypt data and 8 bits to detect errors [1].DES operates on a plain text of 64 bits, which is then divided into 2 parts, left plain text and

right plain text. 16 rounds of encryption are applied to each block. [4]

RSA

RSA stands for Rivest, Shamir and Andelman. This algorithm has been proven to be the most popular and reliable asymmetric algorithm [1] which was designed in 1978. RSA is categorized under integer factorization algorithm [7]. The three steps in the RSA algorithm are the key generation, encryption, and decryption [8]. The plain text and encrypted text in the RSA algorithm fall between 0 and n-1, where n is the product of 2 prime numbers. [10]. Public and private keys are generated using prime numbers [8].

The length of the two prime numbers should be the same. If the value of two prime numbers is small, then the key generated from those two prime numbers will be weak, [8] and this means that the encryption process also becomes weak. By this there is a possible chance of data being cyber-attacked. If the two prime numbers are large, then it becomes more difficult to compute it, it consumes more time and causes degradation in performance [8]. Usually we use two prime numbers, but we can also use 3–4 prime numbers to generate the key, which results in an increase in security.

Diffie-Hellman

Diffie-Hellman algorithm was first introduced in 1976. It is one of the specific methods of exchanging cryptographic keys [1]. In this method, 2 entities or parties jointly make a secret key and share it over an insecure communication channel [1]. This can be done with the help of two prime numbers and a non-zero number. [6].

11. DRAWBACKS OF CRYPTOGRAPHY

Cryptography can only protect the data from possible cyber-attacks, but it can't protect the data from the threats that emerge from the negative layout of the machine [5]

In symmetric encryption there is a major drawback of transmitting the secret key from the sender to the receiver, before even transmitting the real message.

If we add a lot of cryptographic techniques to one set of data, it takes more time for computation and causes the delay.

Sometimes accessing a strongly encrypted, perfectly secured, authentic information becomes difficult for the user at a crucial time.

12. QUANTUM CRYPTOGRAPHY

Quantum cryptography distinguishes itself from other cryptographic schemes by its exclusive reliance on the principles of quantum physics. Unlike classical cryptography, which relies on mathematical techniques to protect encrypted messages from unauthorized access, quantum cryptography operates at the forefront of cryptographic advancements. Its foundation lies deeply in the phenomena of "photon polarization."

As the latest and most advanced branch of cryptography, quantum cryptography leverages the unique properties of quantum particles, such as superposition and entanglement, to achieve secure communication. By utilizing these quantum phenomena, it offers unparalleled levels of security, rendering it virtually impervious to attacks by malicious eavesdroppers.

13. QUANTUM KEY CRYPTOGRAPHY

Unlike classical cryptography schemes, which are solely based on mathematical problems, To achieve improved security, Quantum Key Distribution (QKD) makes use of the basic principles of quantum physics [12]. One unique advantage of QKD is its ability to detect the presence of an eavesdropper. Any attempt made by an eavesdropper to intercept the communication is manifested as errors in the system. This distinguishing feature sets QKD apart from conventional cryptography techniques [13].

The security provided by a QKD system has been rigorously tested and demonstrated to be robust against attacks from adversaries, even in scenarios where the adversary possesses unlimited computational power. This resilience stems from the fundamental principles of quantum mechanics on which QKD is based upon.

14. FUTURE SCOPE OF QUANTUM CRYPTOGRAPHY

Integrating quantum cryptography with the existing communication infrastructure, i.e. by combining it with the basic encryption method – it provides an extra layer of security.

In quantum cryptography, there is a progress from being a theoretical concept to practical implementation.

Researchers are actively engaged in the development of quantum cryptographic systems that aim to achieve improved efficiency and cost-effectiveness.

The advancements in quantum cryptography are expected to pave the way for the adoption of quantum cryptography across diverse industries, including healthcare, defense, and telecommunications.

15. CONCLUSION

In conclusion, the review paper has provided a comprehensive overview of the field of network security and cryptography. The growing reliance on digital networks and communication systems has made network security a crucial concern for both organizations and individuals. Cryptography plays a vital role in protecting sensitive data

and ensuring secure communication channels. Throughout the review, the fundamental concepts and techniques of network security have been explored, including various threat models, types of attacks, and defense mechanisms. The paper also delved into different cryptographic algorithms employed to achieve data confidentiality, integrity, and authentication. Advancements in network security and cryptography have led to the development of robust encryption algorithms, secure key exchange mechanisms, and authentication protocols. Emerging technologies, such as quantum cryptography, have also presented new possibilities for securing digital networks and data.

REFERENCES

[1] Sonia Rani, Harpreet Kaur," Technical Review on Symmetric and Asymmetric Cryptography Algorithms" International Journal of Advanced Research in Computer Science Volume 8, No. 4, May 2017.

[2] Dr. Sandeep Tayal , Dr. Nipin Gupta , Dr. Pankaj Gupta , Deepak Goyal , Monika Goyal," A Review paper on Network Security and Cryptography" Advances in Computational Sciences and Technology ISSN 0973-6107 Volume 10, Number 5 (2017)

[3] Paavni Gaur, Mr. Ajay Kaushik," AES Image Encryption (Advanced Encryption Standard)" International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 9 Issue XII Dec 2021

[4] Nirmaljeet Kaur, Sukhman Sodhi," Data Encryption Standard Algorithm (DES) for Secure Data Transmission" International Journal of Computer Applications (0975 – 8887) International Conference on Advances in Emerging Technology (ICAET 2016)

[5] Prerna Sharma, Khushboo Yadav, Ankit Kumar Tiwari," A Review Paper on Network Security and Cryptography" World Journal of Research and Review (WJRR) Volume-14, Issue-5, May 2022

[6] Muhammad Aamir Panhwar , Sijjad Ali khuhro , Ghazala Panhwar, Kamran Ali memon," SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms" International Journal of Computer Science and Network Security, VOL.19 No.1, January 2019.

[7] Mohd Saiful Adli Mohamad, Roshidi Din, Jasmin Ilyani Ahmad," Research trend review on RSA scheme of asymmetric cryptography techniques" Vol. 10, No. 1, February 2021.

[8] Roopali Sood, Harpreet Kaur," A Literature Review on RSA, DES and AES Encryption Algorithms" in 2023.

[9] Ako Muhamad Abdullah," Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data" June 16, 2017.

[10] Esha Rawat , Anuska Singh, Alap Mahar, Prof. Amit Agarwal," A Review Paper on Cryptography and Network security" May 15, 2022

[11] Gurdeep Singh , Prateek Kumar , Nishant Taneja , Gurpreet Kaur," A RESEARCH PAPER ON CRYPTOGRAPHY" International Journal For Technological Research In Engineering Volume 7, Issue 4, December-2019

[12] Ms. V. Padmavathi, Dr. B. Vishnu Vardhan, Dr. A. V. N. Krishna," Quantum Cryptography and Quantum Key Distribution Protocols: A Survey", 2016 IEEE 6th International Conference on Advanced Computing

[13] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," 2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, Bali, Indonesia, 2018

[14] F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, Nanchang, China, 2015

[15] Firkhan Ali Bin Hamid Ali. (2011). A study of technology in firewall system. 2011 IEEE Symposium on Business, Engineering and Industrial Applications (ISBEIA)