ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

A Review Paper on Computer Network and Cryptography

Ankit Sharma* and Sukhjinder Kaur

Department of Computer Science Engineering,
University School of Engineering & Technology, Rayat Bahra University, Mohali-140 104

Abstract: *Giving security to the information is one of the primary parts of information transmission over wireless network. The Network security not simply expected to give security to end client yet furthermore to the entire Network. Giving security to information is one of the huge problems on the grounds as that the world is moving into digital world. Network security give security to data which is oversee by head. With the quick improvement of computer innovation, computer network keeps on extending the extent of utilization with an ever-increasing number of clients. At many occasions attacks can happen on the network. Nobody needs to deliver their association data or critical information. There are such endless attacks besides, hacking processes in/out your association with the goal of taking your academic information. So here is the need of organization security. This paper momentarily presents the idea of computer network and security, centres on the dangers of network security and examines fundamental methods. It proposes successful measures to further develop the computer network security.*

Keywords: Network Security, Cryptography, Threats.

*Corresponding author: Ankit Sharma
e-mail: anki.sharma333@gmail.com

ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

1. Introduction

Network Security is liable for giving security to every one of the information transits over web from one computer system to another system [1]. With the advancement of time, PC innovation has been incredibly evolved and the present organization correspondence framework has spread to each edge of the world, including political, financial, military and all strolls of public activity [2]. It assumes a critical part. Which cause more unlawful clients to assault and obliterate the organization by utilizing the phony sites, counterfeit mail, Trojan and secondary passage virus simultaneously. Target of the assaults and interruption on the organization are PCs, so when the gate crashers succeed, it will cause many organization PCs in a deadened state likewise, a few trespassers with ulterior intentions view the military and government office as the objective which cause huge dangers for the social and public security [3]. PC Network can be described in to two Peer-to-peer organization and client server network subject to the Administration. The association security is given by an organization director or structure leader. The administrator does the security methodology. The association expected to guarantee an association and the resources got to through the organization from unapproved access. Cryptography is the method involved with changing the privileged information or data into a garbled or mixed structure. Indeed, it is the specialty of composing the message furtively. various feature in information security under cryptography such as data confidentiality, data integrity, authentication, and non-repudiation are integral to modern cryptography [4].

In Fig. 1. sender plain message is to be encrypted into some code structure and afterward unscrambled to the receiver.

2. Computer Network

2.1 Define Network

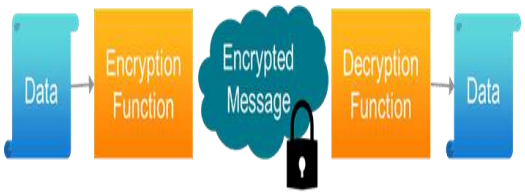

Fig. 1.: Crypto system [8].

Computer Network can be private, for example, inside a organization, and others which may be available to free. An organization has been characterized as any arrangement of interlinking system taking after a net, an organization of streets an interconnected framework, an organization of collusions. A computer network is basically an arrangement of interconnected PCs. PC interconnection can be utilized for a long time, both for organizations and people. For organizations interconnection of PCs utilizing shared server regularly give access to corporate data. Regularly they follow the customer server model. For people, network

ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

offers admittance to an assortment of data and diversion assets [4].

Table 1.: Open System Interconnection (OSI) Model Seven Layers [5].

7. Application Layer
6. Presentation Layer
5. Session Layer
4. Transport Layer
3. Network Layer
2. Data Link Layer
1. Physical Layer

2.3 Open System Interconnection Model

In 1984, a organization known as the International Organization for Standardization (ISO) made a model called the Open Systems Interconnect (OSI). This model characterized rules for interoperability between network makers. An organization could now blend and match network gadgets and conventions from different producers in its own organization without being locked into utilizing a solitary merchant.

Each layer depends upon the organizations gave by the layer under it, directly down to the actual organization hardware, similar to the PC's association interface card, and the wires that interface the cards together. OSI Reference Model describes seven layers of correspondences types, and the interfaces among them [5].

3. Threats in Computer Network

People restless, willing, and qualified to take advantage of each security deficiency, and they diligently search for new experiences and inadequacies.

There are four fundamental classes of threats to arrange security.

1) Unstructured dangers comprise of for the most part unpractised people utilizing effectively accessible hacking instruments like shell contents and secret phrase saltines. Indeed, even unstructured dangers that are just executed with the expectation of testing and testing a programmer's abilities can in any case cause genuine harm to a organization.

2) Structured dangers contrast to unstructured dangers, organized danger programmers are all around experienced and profoundly modern. They use complex hacking instruments to infiltrate organizations and they can break into government or business PCs to extricate data. On specific events, organized dangers are completed by coordinated groups of thugs or industry contenders.

3) External Threats some unapproved individuals outside the organization who don't approach the organization's PC framework or organization could cause outside danger. They generally break into organization by means of the Internet or server. Both experienced and unpractised programmers could present outer dangers.

4) Internal Threats inner dangers happen when somebody has approved admittance to the organization with either a record on a server or actual admittance to the organization. As indicated by the FBI, inner access and abuse represent 60% to 80 percent of detailed occurrences [2].

3.1 Attacks

The dangers utilize an assortment of devices, scripts, and projects to dispatch assaults against organizations and organization gadgets. Regularly, the organization gadgets enduring an onslaught are the endpoints, like servers and work areas. A few sorts of assaults are [4].

- Snooping
- Infections
- IP Spoofing Attacks
- Forswearing of Service

3.2 Vulnerabilities

Malignant clients are consistently lurking in the shadows to slip into networks and make issues and consequently, they unfavourably influence a few organizations all over the planet [10]. A shortcoming that is internet in each organization and gadget. This incorporates switches, work areas, servers, and even security gadgets themselves. Overall terms, framework weakness is a defect or shortcoming in the plan or execution of a data framework. The shortcomings are accessible in the association and individual devices that make up the association. Networks are routinely tortured by one or all of three fundamental shortcomings or inadequacies [4]:

- Innovation
- Setup
- Security strategy

4. Cryptography

4.1 Define Cryptography

Cryptography deals with the certifiable secure of cutting-edge information. Cryptography is the workmanship and investigation of making a cryptosystem that is fit for giving information security. It insinuates the arrangement of contraption subject to arithmetical estimations that give major information security organizations. You can consider cryptography the relationship of a huge device stash contains different strategies in security application [6].

4.2. Services of cryptography

1) Confidentiality: It is a flourishing association that stays aware of the in control from an

ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

unapproved individual. It is sometimes, suggested as security or secret. Secrecy is the essential security administration gave by cryptography. Secrecy can be accomplished through many methods beginning from physical secure to the utilization of arithmetical calculations for data encryption. Secrecy is the crucial security administration given by cryptography. It is a security administration that keeps the data from an unapproved individual.

2) Integrity: The information may get changed by an unlawful substance intentionally or accidently. Decency organization confirm that whether or not data is whole since it was last made, sent, or set aside by a supported customer. Organization that plans with recognize any change to the data. Data uprightness can't hinder the distinction in data, yet gives a method for perceiving whether data has been controlling illegally.

*3) Authentication***:** In data security, confirmation permits to decide if an individual is truly who it professes to be. It affirms the reviver that the information set up has been sent simply by a perceived and set up sender.

Validation administration has two variations –

Message approval perceives the producer of the message with no any regard switch or plan that has sent the message.

Substance check is vowing that data has been gotten from a specific substance, say a requesting site.

4) Non-Repudiation: In non-Repudiation sender of the information can't deny the development or transmission of the said information to a beneficiary. Non-repudiation alludes the guarantee that involved with an agreement or a correspondence can't deny the credibility of their sending of a message or mark on a report that they started. It is a security fix that guarantees that an element can't decline the ownership of a past responsibility or an activity. Non-denial is a property that is for the most part engaging in conditions where there is probability of a dispute over the exchange of data. For example, once an organize is put electronically, a purchaser can't deny the purchase demand, if non-repudiation fix was engaged in this trade [6].

5. Types of cryptography

(1) Symmetric

(2) Asymmetric

1) Symmetric cryptosystem: In Symmetric cryptosystem same keys are used for scrambling and unscrambling the through and through is known as Symmetric Key Encryption. Symmetric cryptosystems are exorbitantly on occasion suggested as secret key cryptosystems.

ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

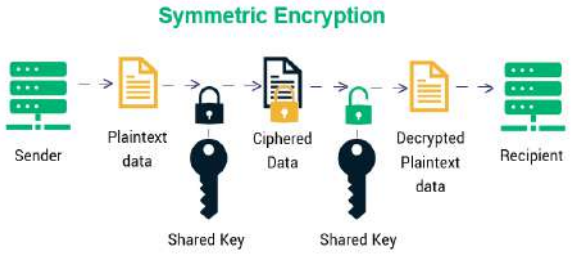

Fig. 2.: Symmetric encryption

Symmetric cryptosystems suggested as symmetric cryptography.

The main elements of cryptosystem base on symmetric key encryption are:

- People by symmetric key encryption should share a standard key before trade of data.
- Keys are discretionary to be changed consistently to forestall any assault on the framework.
- A strong component wants to exist to trade the key between the conveying parties. As keys are important to be changed consistently, this system becomes costly and bulky.

If there should be an occasion of Symmetric Encryption, same cryptography keys are utilized for encryption of plaintext and unscrambling of figure content.

Symmetric key encryption is speedier and less problematic yet their standard disadvantage is essentially both the clients need to move their keys security.

2) Asymmetric cryptosystem communication where not in the least like keys are used for encoding and unscrambling the information is known as asymmetric cryptosystem. In any case, the keys are exceptional, they are all around related and accordingly, recuperate the plaintext by deciphering cipher text is possible. Unbalanced encryption uses two keys and besides known as Public Key Cryptography, since customer uses two keys: public key, which is known to public and a private key which is essentially known to customer [6].

6. Algorithm

The initial and still-most-popular version of public key cryptography, named for the three MIT mathematicians who created it: Ronald Rivest, Leonard Adleman, AdiShamir. Today, RSA is utilised inseveral different software products that can be used for important exchange, electronic signatures, or small-block encryption is a data. A block of encryption with a configurable size is used by RSA. The key-pair comes from a very simple that is the product of two prime numbers produces a big number, n. chosen in accordance with specific guidelines; these primes could Each has 100 or more digits, resulting in a inequivalent to nearly two times the number of prime factors. RSA

ISSN (ONLINE) 2583-2506
http://publications.rayatbahrauniversity.edu.in
RBIJMR-Rayat Bahra International Journal of Multidisciplinary Research, Vol. 02, Issue 01, June 2022

includes three stages: Key Generation, Encryption, and Decryption.

1) *Key Generation Phase*:

Receiver generates a public/private key pair. Algorithm is as follow:

- Select p, q such that p and q both are prime, $p \neq q$
- Calculate $n = p * q$
- Calculate $f(n) = (p - 1)(q - 1)$
- Select integer e such that $\gcd(f(n), e) = 1; 1 < e < f(n)$
- Calculate d such that $d \equiv e\text{-}1 \pmod{f(n)}$
- Public key PUK= (e, n)
- Private key PRK=(d, n)

2*) Encryption Phase*

Encryption is done by sender with receiver's Public Key. Algorithm is as follow:

- Plain Text M is known, $M < n$
- Cipher Text C is calculated as

$$C = M^e \bmod n$$

3*)*

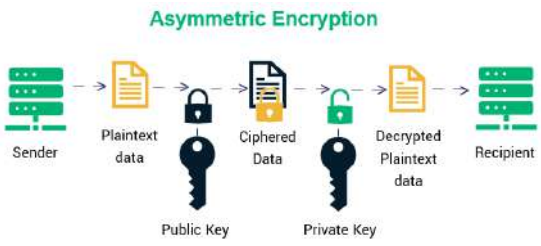

Fig. 3.: Asymmetric encription

Decryption Phase

Decryption is done by receiver using his Private Key. Algorithm is as follow:

- Cipher Text C is known
- Plain Text M is calculated as

$$M = C^d \bmod n$$

7. Five Factor on which Cryptography depends

1) Plain text: The message or information that we want to send secretly. The set of plain text is represented by P.

2) Cipher text: It is the scrambled or unreadable form of information or message. The set of cipher text is represented by C.

3) Key: The rule with the help of which data is scrambled. The set of keys is represented by K.

4) Encryption Function: It is the method using which the cipher text is generated. The set of encryption function is represented by E(x).

5) Decryption Function: It is the inverse function of E(x). It is the effort to generate the original message. The set of decryption function is represented by D(x). Thus, cryptography is depending on {P, C, K, E(x), D(x)} (7)

8. Conclusion

Network security is an imperative variable that numerous associations consider. An assault or danger might reason considerable loss of all together or information to an association. It might likewise obliterate basic foundation. It is, along these lines, the best choice to foster a dependable security strategy for the association's organization. The above network

security arrangements can assume a huge part in relieving the dangers that the firm might insight in its functional climate. All the security approaches ought to guarantee that the data and information are secret without influencing its accessibility or honesty. Scientists ought to totally understand the wellbeing elements to build up sensible destinations and applicable laws and guidelines.

References

[1] K. Sujatha and D. A. Ramya, (2018), A Review on Cryptography and Network Security, Int. J. Pure and Applied Maths., **119 (17)**, pp.1279-1284.

[2] A. Funmilola and A. Oluwafemi, (2015), A Review on Computer Network Security System Network and Complex System, **5(5)**, 40-47.

[3] S. Tayal, N. Gupta, P. Gupta, D, Goyal, M. Goyal, (2017), A Review on network Security and Cryptography, Advances in Comp. Sc. and Tech., **10(5),** pp.763-770.

[4] T. J. Jincy, (2015), Review on Network Security Aspects (Introduction to Vulnerabilities, Threats, and Attacks), Int. J. Engg. Res. Tech. (IJERT), **3(30)**, pp.1-3.

[5] P. Suresh, (2016), Survey on seven layered archit. of OSI model, Int. J. Res. Comp. App. and Robotics, **4(8)**, pp.1-10.

[6] P. Dewangan, (2018), A Review on Network Security and Cryptography.

[7] D. R. Gupta, (2020), A Review on Concepts of Cryptography and Cryptographic Hash Function, Euro. J. Molecular & Clinical Medicine, **7(7)**, pp.3397-3408; O. Awodele, E. E. Onuiri and S. O. Okolie, (2012), Vulnerabilities in network infrastructures and prevention/ containment measures, Proceedings of Informing Science & IT Education Conf. (InSITE).

[8] S. S. Kalluri, (2021), Embedded Security Using Cryptography, Semiengineering.Com, https://Semiengineering.Com/Embedded-Security-Using-Cryptography/.

[9] Sectigostore Staff Types of Encryption, sectigostore.com, April 25, 2020; https://sectigostore.com/blog/types-of-encryption-what-to-know-about-symmetric-vs-asymmetric-encryption/.

[10] Types of Encryption: What to Know About Symmetric vs Asymmetric Encryption - InfoSec Insights (sectigostore.com).

[11] O. Awodele, E. E. Onuiri and S. O. Okolie, (2012), Vulnerabilities in network infrastructures and prevention/ containment measures, Proceedings of Informing Science & IT Edu. Conference (InSITE).

[12] S. N. Kumar, (2015), Review on network security and cryptography, *Int. Transaction of Elect. and Comp. Engg. System*, **3(1)**, pp.1-11.