International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 4172-4176 www.ijaem.net ISSN: 2395-5252

Network Securityand Cryptography: A Review

Souvik Bera[*1], Bratati Roy[*2], Debrupa Pal[*3]
[*1] MCA 2nd year, Computer Application, Narula Institute of Technology, Kolkata, West Bengal, India
[*2] MCA 2nd year, Computer Application, Narula Institute of Technology, Kolkata, West Bengal, India
[*3]Assistant Professor, Computer Application, Narula Institute of Technology, Kolkata, West Bengal, India

Submitted: 25-07-2021 Revised: 04-08-2021 Accepted: 06-08-2021

ABSTRACT
In the era of digitalization, e-commerce applications, and social networks are the most common platforms. So, these organizations around the world are generating huge amounts of data every day and we also have to provide our personal information on numerous platforms. In this situation, data security, as well as network security is the utmost fundamental issue in ensuring the safe transmission of information through the internet. The more users connect with the internet, the more likely high risk of a cyber-attack is to jump. It comprises authorization of access to information that is controlled by the network administrator. It is required to protect not only the computer but the whole network. In this paper, we attempt to review the various network security and cryptographic concepts i.e., the concept to protect the network and data transmission over wireless networks. We also discuss about principles of cryptography in this paper.

Keywords: Network security, cyber-attack, data safety, threats, cryptography

I. INTRODUCTION

Network security is the greater portion of essential components in information security. It is responsible for ensuring all intelligence messages are managed by the networked computer. Network security hand over to all hardware and software functions. This matter can be divided into four closely intricate areas: secrecy, authentication, nonrepudiation, and integrity control. the secrecy that means keep secret. Secrecy has to do with keeping secret the intelligence message from unauthorized users. Authentication is the method of acceptance of a user's identity. In security system authentication verifying the identity as a user, devise to allowing access to declaring sensitive information [1].

Cryptography means 'secret communication'. This is an outbound technology, which is significant for network security. Cryptography, the inquiry of systems for secure concurrence. It is helpful for examining those conferences, that are identified with different viewpoints, alignment, of information, non-denial, and information's impartiality. Computer systems and networks that are strong, processing and communicating sensitive or valuable information require protection against such unauthorized access [1].Cryptography is the science of communicating in hidden code. In a broader sense, it is about generating and analyzing protocols that block adversaries [2].

Testing is the way to efficiently share scuffled information. Encode message with an unequivocally secure key which is known just by sending and the beneficiary end is a noteworthy perspective to get strong security in sensor to organize. The safe dealings of key between sender and receiver are a lot of tormenting message in asset compulsory sensor arrange. The information ought to be scrambled first by clients before it is outsourced to a remote distributed storage benefit and both information security [3] when the client wants the realization of some paragraph of the entire information, and the client exigent to the realization of a few sections of the whole information, the distributed storage framework will give the availability without recognizing what the segment of the encoded information comes back to the client is about.

II. LITERATURE SURVEY

a. Network Security Model

Figure 1 indicates the model of system security. A message is to be commute starting with one gathering then onto the next over some kind of internet administration. A third party may be responsible for distributing the secret to the sender and receiver while keeping it from any rival. Security perspectives come into play when it is necessary or desirable to protect the information transmission from a competing who may present a threat to secrecy, truth, and so on. Procedures for furnishing security have two constituents [4].

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 4172-4176 www.ijaem.net ISSN: 2395-5252

- A secured change on the data to be sent. The message ought to be encrypted by key with the objective that is confused by the adversary.
- An encryption key applied in association with the transformation to encrypt the message before transmission and decrypt it at the receiving end.

b. Need for key management in the cloud

Encryption offers information security while key administration authorizes access to guaranteed information.Information should be encoded in transit, and on reinforcement media.Both encryption and key management are vital to assist secure applications and information kept in the cloud [5]. Preconditions of feasible key management are discussed below:

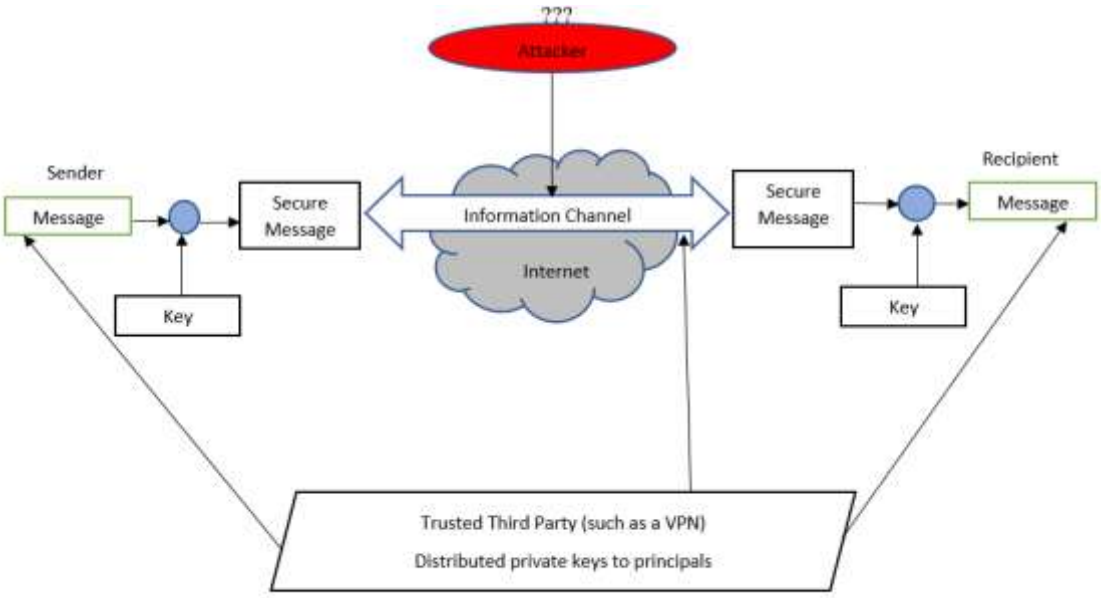

Figure 1: System Security Model

1. **Safe digital store** - The digital store must be protected from harmful clients. A harmful client tried to accesses the keys so that they can retrieve the encrypted information. Hence the digital stores must be protected.
2. **Access to digital store-** Access to the digital store should be restricted to the customers that have the right to get the information. The substance that uses a given key should not be the element that stores the key.
3. **Key backup and recoverability**-Keys need secure reinforcement and recuperation measures.Cloud providers require to assure that keys aren't lost via reinforcement and recuperation constituents.

III. CRYPTOGRAPHIC TECHNIQUES

Cryptography is an approach to transmitting information in a specific frame so that the intended receiver can read and process it.The term is frequently linked with transforming plaintext message (referred as cleartext) into ciphertext (known as encryption), then back once more (known as decryption) [6].

Key: A key is a piece of information that can be numeric or alphanumeric when processed through a cryptographic algorithm, can encode or decode cryptographic data.

Plaintext - Unencrypted information that is the input to a crypto system. For example, a boy named Alice needs to send a "Hello Friend how are you" message to a boy named Bob. Here "Hello Friend how are you" is a plaintext.

Ciphertext - Ciphertext- Encrypted text obtained as a result of applying encryption algorithm on the plaintext. For ex, "Ajd672#@91ukl8*^5%" is a ciphertext generated for "Hello Friend how are you". It is different from code text as the latter is an output of a code, not a cipher.

Encryption- It is the technique of encoding the information. This technique transforms the original information, called plaintext into another type known as ciphertext. The goal is that only the intended recipient can decipher a ciphertext back to plaintext and access the original information.

Decryption- A turnaround technique of encryption is known as decryption. In this procedure, cipher

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 4172-4176 www.ijaem.net ISSN: 2395-5252

text is transformed into plain content. The decoding process needs two things-a deciphering calculation and a key. Calculation implies the technique that has been applied as a part of decryption. Broadly, both calculations are the same.

IV. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Primarily there are two varieties of methods that are employed for encryption and decryption data, they are

Symmetric key cryptography

Asymmetric key cryptography

Symmetric Key Cryptography

It is a kind of encryption where a single key is used for encryption and decryption of electronic information. By applying symmetric encryption algorithms, data is converted to a form that cannot be understood by anyone who does not possess the secret key to decrypt itIt is prompt and effective for large amounts of data [7].

Asymmetric Key Cryptography

It is a kind of encryption where a pair of related keys are used- one public key and another private key for encryption and decryption of a message and preserve it from unauthorized access or use.A private key, also

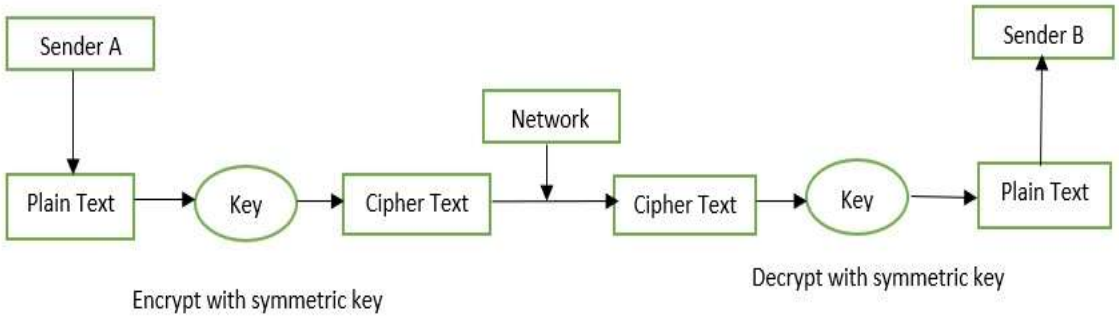

Figure 2: Symmetric Key Cryptography

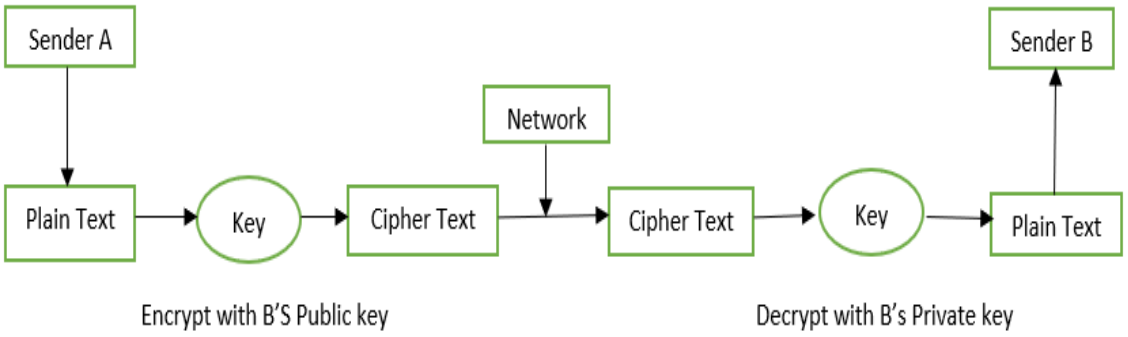

Figure 3: Asymmetric Key Cryptography

called secret key is shared only with key's initiator.This encryption utilizes longer keys for providing improved security. However longer key length slower encryption speed [8].

Digital Signature

The digital signature is the public key fundamentals of message authentication. It ensures that the contents of a message have not been modified in transit. By applying digital signature, message is encrypted with the sender's private key and can be verified by anyone who has access to the private key, and therefore is likely to assure the security of the network [9].

V. ADVANCED ENCRYPTION ALGORITHM

The AES algorithm is a symmetrical block cipher algorithm which takes plain text of 128 bits as input and transform them to ciphertext applying 128, 192 and 256 bits. It is an iterative and worldwide secured standard. It is based on 'substitution–permutation network'. It consists of a series of linked operations, some of which include replacing inputs by specific outputs (substitutions)

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 7 July 2021, pp: 4172-4176 www.ijaem.net ISSN: 2395-5252

and others involve shuffling bits around (permutations).

Effective implementation of AES

With the fast movement of computerized information trade in electronic route, in information stockpiling and transmission, data security is turning out to be a good deal. An answer is available for cryptography which is considered a vital part in data security structure against different assaults.

With the rapid movement of automated information via electronic medium and online transactions, data security has become a vital issue. A solution is available in cryptography that supposes a vital part in data security infrastructure towards various attacks. Several calculations are applied as a component of this security system uses to encode information that can be decoded by applying the associated key . Two sorts of cryptographic approaches are being utilized: symmetric and hilter kilter. In this paper, we have utilized symmetric cryptographic approach AES (Advanced encryption standard) having 200 pieces obstruct and additional key size. Applying 5*5 Matrix AES calculation is executed for 200 pieces. On executing, the suggested work is contrasted and 256 pieces, 192 bits, and 128 bits AES systems on two focuses. These focuses are encryption and decryption time and throughput at both sender and receiver sides [10].

Open key encryption in which a message is encrypted with a beneficiary's public key. The message can't be decrypted by any individual who does not have the coordinating private key, who is dared to be the proprietor of that key and the individual related with general society key. This is an attempt to guarantee classification.

Efficient Data Hiding by Using AES & Advance Hill Cipher Algorithm

In this paper we recommend a concealed information technique employing AES computation. Two widely used strategies for transmitting fundamental data secretly are Steganography and Cryptography. For making information protected cryptography was introduced. Cryptography can't provide an advanced security technique in light of the fact that the mixed message is still available to the spy. Requirement for Information security arises. By combining cryptography and steganography, security can be improved. Several cryptography strategies are available;however, AES is an outstanding amongst the most helpful procedures. Themessage is encrypted by the usage of AES calculation for encoding messages utilizing 128-piece key [11].

VI. COMPARISION OF SEVERAL ENCRYPTION ALGORITHM

In Table 1, comparative analysis of several encryption algorithms based on their capability to secure and preserve data against attacks and speed of encryption and decryption [12].

SYMMETRIC KEY CRYPTOGRAPHY	SIZE OF KEY	IN STEPS OF
DES	40 -56 bits	8 bits
Triple-DES (two key)	64- 112 bits	8 bits
Triple -DES (three key)	120-168 bits	8 bits
PUBLICKEY CRYPTOGRAPHY		
Diffie -Hellman	512-2048 bits	64 bits
RSA	512-2048 bits	64 bits
DIGITAL SIGNATURE		
DSA	512-2048 bits	64 bits
RSA	512-2048 bits	64 bits

Table 1: Comparison of Encryptions

VII. CONCLUSION

Information security safeguards the information from unauthorized access. Client information security is a vital issue over cloud. Information security allows the secure operation of applications implemented on the organization's IT systems. Cryptographic techniques are becoming more adaptable and various keys are used for encryption and decryption of data. Encoding the message with a secure key that is known at the sender's and receiver's end provides great security.

The paper revealed several techniques that are applied as a part of cryptography for network security. The administration of keys protects information from unauthorised access. Similarly, it can verify the genuineness of the transmitted message.

REFERENCES

[1]. Marin, Gerald A. "Network security basics." IEEE security & privacy 3.6 (2005): 68-72.

[2]. Stinson, Douglas Robert, and Maura Paterson. Cryptography: theory and practice. CRC press, 2018.

[3]. Devi, T. Rajani. "Importance of cryptography in network security." 2013 International conference on communication systems and network technologies. IEEE, 2013.

[4]. Daya, Bhavya. "Network security: History, importance, and future." University of Florida Department of Electrical and Computer Engineering 4 (2013).

[5]. Buchade, Amar Ramesh, and Rajesh Ingle. "Key management for cloud data storage: methods and comparisons." 2014 Fourth International Conference on Advanced Computing & Communication Technologies. IEEE, 2014.

[6]. Devi, T. Rajani. "Importance of cryptography in network security." 2013 International conference on communication systems and network technologies. IEEE, 2013.

[7]. Delfs, Hans, and Helmut Knebl. "Symmetric-key cryptography." Introduction to Cryptography. Springer, Berlin, Heidelberg, 2015. 11-48.

[8]. Turner, Sean. Asymmetric Key Packages. RFC 5958, August, 2010.

[9]. Kaur, Ravneet, and Amandeep Kaur. "Digital signature." 2012 International Conference on Computing Sciences. IEEE, 2012.

[10]. Zhang, Xinmiao, and Keshab K. Parhi. "Implementation approaches for the advanced encryption standard algorithm." IEEE Circuits and systems Magazine 2.4 (2002): 24-46.

[11]. Choudhary, Kajal, Virendra Choudhary, and Hitesh Daiya. "Network Security with Cryptography." TECH TONICS: 20.

[12]. Andriani, Ria, Stevi EmaWijayanti, and Ferry Wahyu Wibowo. "Comparision Of AES 128-, 192- And 256-Bit Algorithm for Encryption and Description File." 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE). IEEE, 2018.