Cryptographic Data Encryption and Decryption for Secure data Transfer towards Network Security

Gangadhar
M.Tech Scholar, Department of CSE,
BABA Institute of Technology and Sciences , AP

J Ratna Kumar.
Assoc.Prof, Department of CSE,
BABA Institute of Technology and Sciences, AP.

Abstract: Network Security and Cryptography is an idea to ensure Network and information transmission over remote Network. Information Security is the fundamental part of secure information transmission over inconsistent Network. Network security includes the approval of access to information in a Network, which is controlled by the Network overseer. Clients pick or are allocated an ID and secret word or other confirming data that permits them access to data and projects inside their power. Network security covers an assortment of PC Networks, both open and private, that are utilized in regular employments leading exchanges and interchanges among organizations, government offices and people. Networks can be private, for example, inside an organization, and others which may be available to free. Network security is associated with associations, endeavors, and different sorts of establishments. In this paper we additionally contemplated cryptography alongside its standards. Cryptographic frameworks with figures are portrayed. The cryptographic models and calculations are laid out.

Keywords: Network Security, Cryptography, Security Challenges.

I. Introduction

Network Security is the most indispensable part in data security since it is in charge of anchoring all data went through arranged PCs. Network Security alludes to all equipment and programming capacities, attributes, highlights, operational methodology, responsibility, measures, get to control, and regulatory and the board arrangement required to give a worthy dimension of insurance for Hardware and Software , and data in a network.Network security issues can be partitioned generally into four intently entwined regions: mystery, validation, nonrepudiation, and trustworthiness control. Mystery, additionally called classification, has to do with keeping data out of the hands of unapproved clients. This is the thing that typically rings a bell when individuals consider arrange security. Confirmation manages deciding whom you are conversing with before uncovering touchy data or going into a business bargain. Nonrepudiation manages marks. Message Integrity: Even if the sender and beneficiary can verify one another, they additionally need to protect that the substance of their correspondence isn't changed, either malicously or unintentionally, in transmission. Expansions to the checksumming procedures that we experienced in dependable transport and information interface conventions. Cryptography is a developing innovation, which is vital for Network security. The far reaching utilization of modernized information stockpiling, preparing and transmission makes touchy, important and individual data powerless against unapproved get to while away or transmission. Because of proceeding with headways in correspondences and listening in advances, business associations and private people are starting to secure their data in PC frameworks and Networks utilizing cryptographic strategies, which , until as of late, were solely utilized by the military and discretionary networks. Cryptography is a fundamental of the present PC and correspondences Networks, shielding everything from business email to bank exchanges and web

shopping While established and current cryptography utilize different numerical methods to maintain a strategic distance from spies from taking in the substance of scrambled messages. PC frameworks and Networks which are putting away, preparing and conveying delicate or important data require security against such unapproved access[1]. The main general way to deal with sending and putting away information over media which are shaky is to utilize some type of encryption. An essential concern is that numerous assaults include mystery way access to data assets, and associations are regularly uninformed of unapproved access to their data frameworks. Thus the quantum cryptography utilized. The security of quantum cryptography keeps up in its capacity to trade the encryption key with supreme security. Cryptography has its root in the old world. As per [7], the Julius Caesar utilized straightforward cryptography to shroud the importance of his messages. As indicated by [7], The Caesar figure is a monoalphabetic Cryptosystem, since it replaces each given plain content letter, wherever in the first message it happens, by a similar letter of the figure content letters in order. Anyway the ideas of source and beneficiary, and channel codes are present day thoughts that have their underlying foundations in the data hypothesis. Claude Shannon, in the 1948 gave the data hypothesis premise to mystery, which characterizes that the measure of vulnerability that can be brought into an encoded message can't be more noteworthy than that of the cryptographic key used to encode it [9]. Claude Shannon displayed this idea of security in interchanges in 1949, it suggests that an encryption plot is consummately secure if, for any two messages M 1 and M 2, any figure content C has a similar likelihood of being the encryption of M 1 just like the encryption of M 2 [6]. Shannon was produced two vital cryptographic ideas: disarray and dissemination. As indicated by Salomon [8], the term disarray intends to any strategy that makes the factual connection between the figure content and the key as troublesome as could be allowed, and dispersion is a general term for any encryption method that extends the measurable properties of the plaintext over a scope of bits of the figure content.

II. Related work

Shouhuai Xu et. al.[1] proposed new complex frameworks that can be produced by misusing trust based interpersonal organizations, (for example, Facebook) to store secured information in an appropriated way, utilizing edge cryptography, to build up certain useful characteristics. Lo-Yao Yeh et. al.[2] talk about distributed online informal organizations that are at present helpless without a strong cluster validation technique. Three new conventions are proposed, including one way hash work, intermediary encryption, and endorsements as basic cryptosystems. These have bring down computational expense than the standard techniques. Ralf Kusters et. al.[3] examine the issue of building up a standard structure of cryptographic confirmation of Java and Java like projects which are as yet open. The strategic distance properties of Java like projects can be utilized to give cryptographic certifications; specifically, computational in noticeability, utilizing recreation based security. This is accomplished utilizing another all-encompassing dialect called Jinja+ , which reaches out from Jinja. Jinja gives significant Java usefulness. It is utilized to give the system to cryptographic confirmation required. Idoia Aguirre et. al.[4] clarify a run of the mill situation in any corporate system where the system security examiners autonomously settle on proper measures to react to security cautions. This paper proposes a structure for Security data and occasion administrators (SIEMs) of various spaces to cooperatively settle on choices in light of security dangers which enhances security parts of the corporate system and in the meantime fundamentally diminishing the remaining task at hand. Mai Abdelhakim et. al.[5] talk about Byzantine adaptation to internal failure which is a subfield of adaptation to non-critical failure motivated by the well known two officers' concern where a little blame in the underlying stages can expand into a progressively mind boggling and muddled issue. The proposed arrangement in this paper is the q-out-of-m rule which is prevalent in appropriated location and can accomplish a decent tradeoff between miss discovery likelihood and false caution rate in a PC organize, which functions accordingly: 'm' arbitrary sensors are

surveyed, and in the event that 'q' of them report 1, the framework reportsthe focus as present. Notwithstanding, this plan is unfeasible for expansive systems because of high computational multifaceted nature; along these lines, this paper shows a direct q-out-of-m plot that can be effortlessly connected to extensive systems. The paper likewise proposes a successful malignant hub discovery plot and gives reproduction guides to show the execution of proposed approaches. Geetha et. al.[6] talk about Mobile Agent which is a program that moves from host to have playing out an explicit assignment. Trust and Reputation Management is a notoriety based framework where each host has a trust and notoriety file. A safe way can be set up utilizing TRM for Mobile Agents, enabling a few standard assaults to be stayed away from and organizing with remote hosts to be protected and secure. Jesus Tellez Isaac et. al.[7] clarify about the expansion of portable frameworks being utilized for installments has cleared approach to uncover certain security vulnerabilities. Cash exchange can happen through cell phones by means of SMS, GPRS, RFID and so on and are looked with certain security issues. One of the principle issues is that the keys created by the general population key cryptography method are excessively expansive and increases to the overhead. Another sort of cryptography is presented, Elliptic Curve Cryptography (ECC), which help evade this specific issue. The paper talks about another steady issue which is limited web network wherein the trader has no web access at the season of installment which opens the framework to security dangers. The paper closes by pointing out that m-installment client and m-installment exchanges will see a hazardous development in the up and coming years and security in these m-exchanges will remain a vital issue.

II. Cryptographic Principles

A. *Redundancy*

Cryptographic principle 1: The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message. Messages must contain some redundancy.

B. *Freshness*

Cryptographic principle 2: Some method is needed to foil replay attacks. One such measure is including in every message a timestamp valid only for, say, 10 seconds. The receiver can then just keep messages around for 10 seconds, to compare newly arrived messages to previous ones to filter out duplicates. Messages older than 10 seconds can be thrown out, since any replays sent more than 10 seconds later will be rejected as too old.

III. Cryptosystem Types

In general cryptosystem are taxonomies into two classes, symmetric or asymmetric, depending only on whether the

keys at the transmitter and receiver are easily computed from each other. In asymmetric cryptography algorithm a different key is used for encryption and decryption. In the symmetric encryption, Alice and Bob can share the same key (K), which is unknown to the attacker, and uses it to encrypt and decrypt their communications channel.

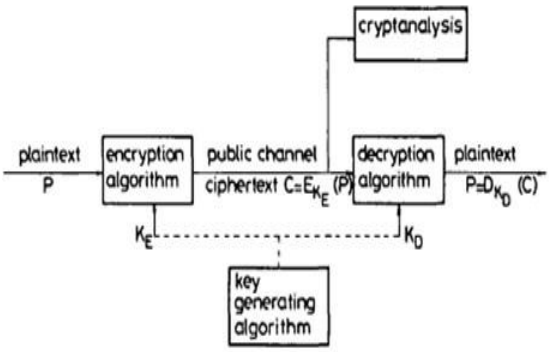

Fig. 1 General secrecy Network

Cryptographic Networks are used to provide privacy and authentication in computer and communication Networks. As

shown in Fig. 1, encryption algorithms encipher the plaintext, or clear messages, into unintelligible ciphertext or cryptograms using a key. A deciphering algorithm is used for decryption or decipherment in order to restore the original information. Ciphers are cryptographic algorithms; cryptography is the science of secret communications; cryptanalysis is the science of breaking ciphers; and cryptology is the science of cryptography and cryptanalysis. Cryptosystems are either symmetric, in which case both the enciphering and deciphering keys must be kept secret, or asymmetric, in which case one of the keys can be made public without compromising the other.

A. Asymmetric Cryptosystems

There are practical problems associated with the generation, distribution and protection of a large number of keys. A solution to this key-distribution problem was suggested by Diffie and Hellman in 1976 [10]. A type of cipher was proposed which uses two different keys: one key used for enciphering can be made public, while the other, used for deciphering, is kept secret. The two keys are generated such that it is computationally infeasible to find the secret key from the public key. If user A wants to communicate with user B, A can use B's public key (from a public directory) to encipher the data. Only B can decipher the ciphertext since he alone possesses the secret deciphering key. The scheme described above is called a public-key Cryptosystem or an asymmetric Cryptosystem[11]. If asymmetric algorithms satisfy certain restrictions, they can also be used for generating so-called digital signatures[12].

B. Symmetric Cryptosystems

In symmetric Cryptosystems (also called conventional, secret-key or one-key Cryptosystems), the enciphering and deciphering keys are either identical or simply related, i.e. 684 *IEE PROCEEDINGS, Vol. 131, Pt. F, No. 7, DECEMBER 1984* one of them can be easily derived from the other. Both keys must be kept secret, and if either is compromised further secure communication is impossible. Keys need to be exchanged between users, often over a slow secure channel, for example a private courier, and the number of keys can be very large, if every pair of users requires a different key, even for a moderate number of users, i.e. $n(n - 1)/2$ for n users. This creates a key-distribution problem which is partially solved in the asymmetric Networks. Examples of symmetric Networks are the data encryption standard (DES) [4] and rotor ciphers.

IV. Cryptographic Model and Algorithm

A. *Encryption model*

There are two encryption models namely they are as follows: Symmetric encryption and Asymmetric encryption. In

Symmetric encryption,

Encryption key = Decryption key. In Asymmetric encryption, Encryption key ¹ Decryption key.

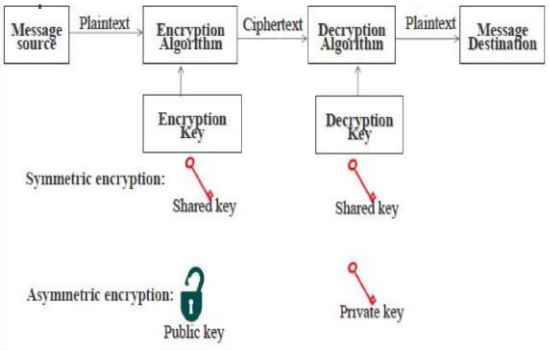

Fig 2: Cryptography

B. *Algorithm*

There are of course a wide range of cryptographic algorithms in use. The following are amongst the most well-known:

1) *DES:* This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' Network. Further Details on the DES Algorithm.

2) *RSA:* RSA is a public-key Network designed by Rivest, Shamir, and Adleman. Further Details on the RSA Algorithm.

3) *HASH:* A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.

4) *MD5:* MD5 is a 128 bit message digest function. It was developed by Ron Rivest. Further Details on the MD5 Algorithm.

5) *AES:* This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.

6) *SHA-1:* SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason SHA-1 is recommended in preference to MD5.

7) *HMAC:* HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

V. Different Types of Security Attacks

A. Passive Attacks

Passive attacks break the whole Network using observed data. For Example, sender and receiver both have plain text of data which is already known to the attacker. Some properties of Passive Attacks:

I. Interception: It involves accessing the data of an email and making it available to someone other than the sender or intended recipient. It also called "Man in the middle" attack.

II. Traffic analysis: This technique that look like communication pattern between entities in a Network.

B. Active Attacks

In this attack the attacker sends data to both sender and receiver or sometimes completely cut off the data stream.

Active attack has some properties:

I. Interruption: Attacker prevents the original sender to access the site. It attacks the availability called DOS attack.

II. Modification: Information is transmitted in plain text. Attacker mostly changes data during transmission.

III. Fabrication: Without authentication attacker create false account or items.

C. DOS Attack

In network security DOS attack is major issue. If anyone has basic knowledge of security then he can easily launch the attack on network. Other attacks take more time but this attack does not take more time and plan to execute. DOS attack is very powerful it can be shutdown company network. The main task of this attack is checking availability and continuously sends the request over network. Triton is network tool which is available on internet. It is mainly used for attack any network. Bandwidth, TCP connection, CPU cycle is main part of network for attack. Zombies are a network of multiple users in a same network where this attack is initiated. Computer is infected by these attacks but users are unaware of this thing.

VI. Proposed Methodology

There are many ways of classifying data cryptographic algorithms but for the purpose of this paper, they will be classified based on the number of keys that are employed for encryption and decryption. The SKC method uses only a single key for both encryption and decryption. The schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing while block cipher scheme encrypts one block of data at a time using the same key on each block. The main drawback of this method is propagation error because a distorted bit in transmission will result in n distorted bits at the receiving side. Though stream ciphers do not propagate transmission errors, they are periodic therefore the key-stream will eventually repeat. This normally results in the use of digital signature mechanisms with either large keys for the public verification function or the use of a TTP. PKC

scheme uses one key for encryption and a different key for decryption. Modern PKC was first described using a two-key crypto Network in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key [5]. In PKC, one of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. RSA is one of the first and still most common PKC implementation that is in use today for key exchange or digital signatures. The cardinal advantage of this method is that administration of keys on a network requires the presence of only a functionally trusted TTP, as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner, as opposed to in real time. Many public-key schemes yield relatively efficient signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart [6-9]. The HF uses a mathematical transformation to irreversibly "encrypt" information. This algorithm does not use keys for encryption and decryption of data. It rather uses a fixed-length hash value which computed based on a plaintext that makes it impossible for either the contents or length of the plaintext to be recovered. These algorithms are typically used to provide a digital fingerprint of a file's content, often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating Networks to encrypt passwords to provide some measure of the integrity of a file.

VII. Conclusion

The paper has presented data encryption and decryption in a network environment that was successfully implemented. With this software, data can be transferred from one computer terminal to another via an unsecured network environment. An eavesdropper that breaks into the message will return a meaningless message. Obviously encryption and decryption is one of the best ways of hiding the meanings of a message from intruders in a network environment.

References

[1]. W. Stallings, Cryptography and Network Security Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2009.

[2]. Himani Agrawal and Monisha Sharma, "Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology Vol.3, No.12, 2012.

[3]. Manoj Kumar Pandey, et.all., "Survey Paper: Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Vol.2, No.12, 2013.

[4]. Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[5]. "File Encryption and Decryption Using Secure RSA", Rajan.S. Jamgekar, GeetaShantanu Joshi, International Journal of Emerging Science and Engineering (IJESE)ISSN: 2319–6378, Vol.1, No.4, 2013.

[6]. "ElGamal Digital Signature Algorithm of Adding a Random Number", Xiaofei Li, Xuanjing Shen and Haipeng Chen, College of Computer Science and Technology, Jilin University, Changchun, China, Journal Of Networks, Vol.6, No.5, 2011

[7] http://en.wikipedia.org/wiki/Information_security

[8] M. S. Lew, N. Sebe, C. Djeraba, and R. Jain, "Content- based multimedia information retrieval:p state of the art and challenges," ACM Trans. Multimedia Comput, Feb. 2006.

[9] Harikrishna Narasimhan, Sanjeev Satheesh, "A Randomized Itersative Improvement Algorithm for Photomosaic Generation", Vol 2,April 2010.

[10]http://www.utica.edu/faculty_staff/qma/needforsecurity.pdf