International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Review on Network Security and Cryptography

Sandeep Kaur, Raghbir Kaur, C. K. Raina

Computer Science Department, AIT, Chandigarh, Kharar, Punjab, India

ABSTRACT

On the internet with the advent of world wide web, world generate a large amount of data daily. Data security is use for safe the information through the internet. Also network security issues are now becoming important as society is moving towards digital information age. As more and more users connect to the internet it attracts a lot of cyber-criminals. It comprises authorization of access to information in a network, controlled by the network administrator. The task of network security not only requires ensuring the security of end systems but of the entire network. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts. This paper discusses the state of the art for a broad range of cryptographic algorithms that are used in networking applications.

Keywords : Network Security, Cryptography, Decryption, Encryption

I. INTRODUCTION

Internet has become more and more widespread, if an unauthorized person is able to get access to this network, he can not only spy on us but he can easily mess up our lives. Network Security & Cryptography is a concept to protect network and data transmission over wireless network.All components work together to increase the overall security of the computer network. Security of data can be done by a technique called cryptography. So one can say that cryptography is an emerging technology,

The key formed by neural network is in the form of weights and neuronal functions which is difficult to break..

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Cryptography is the science of writing in secret code. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. The development of the World Wide Web resulted in broad use of cryptography for e-commerce and business applications. Techniques used for decrypting a message without any knowledge of the encryption details fall into the area of cryptanalysis. Cryptanalysis is what the layperson calls “breaking the code.”

II. Types of Security Attacks

Passive Attacks:- This type of attacks 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 an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic patten

Release of Message Contents: Read contents of message from sender to receiver.

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 that 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.

III. Security Services

It is a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. It enhances the security of data processing and transferring.

Data Integrity:- It can apply to a stream of messages, a single message, or selected fields within a message. A loss of integrity is the unauthorized modification or destruction of information.

Data Confidentiality:- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Authenticity:- Provide authentication to all the node and base station for utilizing the available limited resources. It also ensures that only the authorized node can participant for the communication.

Access Control:- Access control is the ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

IV. Network Security Model

Figure shows the model of network security. A message is to be transferred from one party to another across some sort of Internet service. A third party may be responsible for distributing the secret information to the sender and receiver while keeping it from any opponent. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:-International Transaction of Electrical and Computer Engineers System

• A security-related transformation on the information to be sent. Message should be encrypted by key so that it is unreadable by the opponent. • An encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

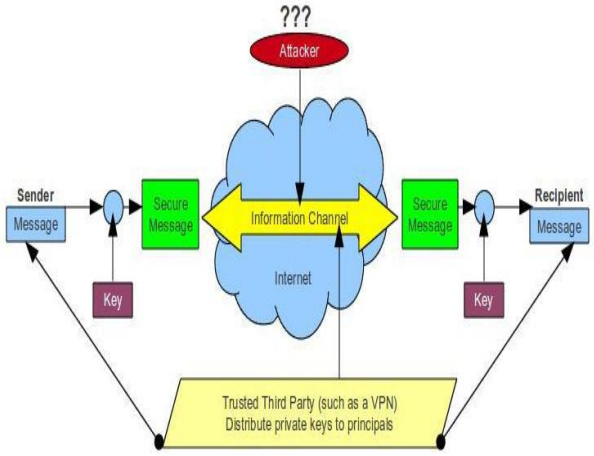


Figure 1. Model for network security

Need for Key Management in Cloud :- Encryption provides data protection while key management enables access to protected data. It is strongly recommended to encrypt data in transit over networks, at rest, and on backup media. Both encryption and key management are very important to help secure applications and data stored in the Cloud. Requirements of effective key management are discuss below.

• **Secure key stores:** The key stores themselves must be protected from malicious users. If a malicious user gains access to the keys, they will then be able to access any encrypted data the key is corresponded to. Hence the key stores themselves must be protected in storage, in transit and on backup media.

Access to key stores: Access to the key stores should be limited to the users that have the rights to access data. Separation of roles should be used to help control access. The entity that uses a given key should not be the entity that stores the key

Key backup and recoverability: Keys need secure backup and recovery solutions. Loss of keys, although effective for destroying access to data, can be highly devastating to a business and Cloud providers need to ensure that keys aren't lost through backup and recovery mechanisms

V. Cryptography Mechanism

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext message into ciphertext (a process called **encryption**), then back again (known as **decryption**). There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (symmetric) cryptography, public-key (or asymmetric) cryptograpy, each of which is described below.

Secret Key Cryptography:-With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure, 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 to decrypt the cipher text C and recover the plaintext message M. Because a single key is used for both functions, secret key cryptography is also called **symmetric encryption**. With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.

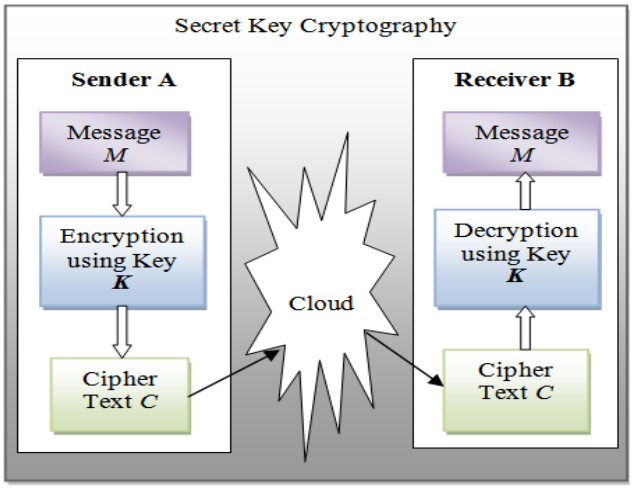


Figure 2. Secret key cryptography

Secret key cryptography 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. 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 ciphertext in a stream cipher. Block ciphers can operate in one of several modes; the following four are the most important:

• **Electronic Codebook (ECB) :-** mode is the simplest, most obvious application: the secret key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common 4 International Transaction of Electrical and Computer Engineers System

• **Cipher Block Chaining (CBC):-** mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous ciphertext block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.

• **Cipher Feedback (CFB):-** mode is a block cipher implementation 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. If we were using 1-byte CFB mode, for example, each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted.

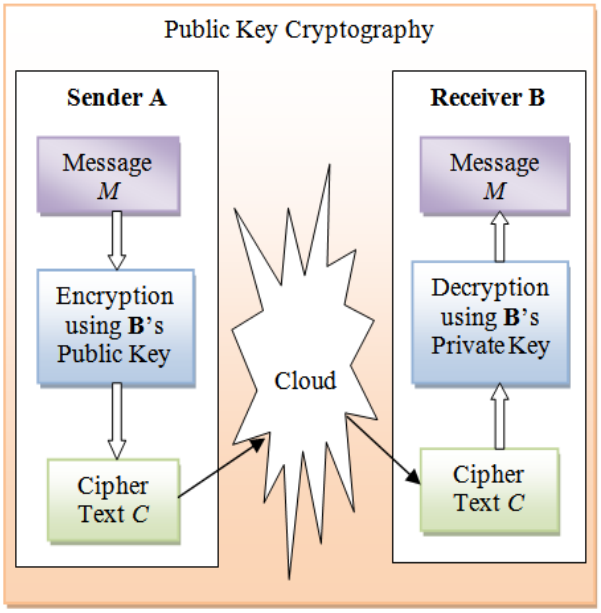
Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams. Stream ciphers come in several flavors but two are worth mentioning here. **Self-synchronizing stream ciphers** calculate each bit in the keystream as a function of the previous n bits in the keystream **Synchronous stream ciphers** generate the keystream in a fashion independent of the message stream but by using the same keystream geration function at sender and receiver. Secret key cryptography algorithms that are in use today include:

• **Data Encryption Standard (DES):** DES is a block-cipher employing a 56-bit key that operates on 64-bit blocks. DES algorithm as described by Davis R. takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into cipher text bit string of the same length. 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time.

• **Advanced Encryption Standard (AES):** AES [7,8] is a block cipher intended to replace DES for commercial applications. It uses a 128-bit block size and a key size of 128, 192, or 256 bits. The number of internal rounds of the cipher is a function of the key length. The number of rounds for 128- bit key is 10.

Public-Key Cryptography :-

Public-key cryptography is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a **public key** and one a **private key**. These keys are mathematically related although knowledge of one key does not allow someone to easily determine the other key. As shown in Figure ,the sender A uses the public key of receiver B (or some set of rules) to encrypt the plaintext message M and sends the ciphertext C to the receiver. The receiver applies own private key (or ruleset) to decrypt the cipher text C and recover the plaintext message M. Because pair of keys is required, this approach is also called **asymmetric cryptography**.



6. Network and Internet Security:- Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Types of Network Security:

Wireless Network Security:- Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (**WEP**) and Wi-Fi Protected Access (**WPA**). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WAP security is primarily provided by the Wireless Transport Layer Security (WTLS), which provides security services between the mobile device (client) and the WAP gateway to the Internet. There are several approaches to WAP end-to-end security. Two important WTLS concepts are the secure session and

the secure connection, which are defined in the specification as:

1) **Secure connection:-** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. Between any pair of parties (applications such as HTTP on client and server), there may be multiple secure connections. In theory, there may also be multiple simultaneous sessions between parties, but this feature is not used in practice.

2) **Secure session:-** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters, which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection. There are a number of states associated with each session. Once a session is established, there is a current operating state for both read and write (i.e., receive and send). In addition, during the Handshake Protocol, pending read and write states are created. Upon successful conclusion of the Handshake Protocol, the pending states become the current states.

Electronic Mail Security:- Email is vulnerable to both passive and active attacks. The protection of email from unauthorized access and inspection is known as electronic privacy. In countries with a constitutional guarantee of the secrecy of correspondence, email is equated with letters and thus legally protected from all forms of eavesdropping. With the explosively growing reliance on e-mail, there grows a demand for authentication and confidentiality services. Two schemes stand out as approaches that enjoy widespread use: Pretty Good Privacy (**PGP**) and Secure/Multipurpose Internet Mail Extension **S/MIME**. PGP is an open-source, freely available software package for e-mail security. PGP incorporates tools for developing a public-key trust model and public-key certificate management.
S/MIME is an Internet standard approach to e-mail security that incorporates the same functionality as PGP. It is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security.

VI. CONCLUSION AND FUTURE WORK

With the explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose internal private network is connected to the Internet. The security for the data has become highly important. User's data privacy is a central question over cloud. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. The paper presented various schemes which are used in cryptography for Network security purpose. Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret International Transaction of Electrical and Computer Engineers System 11. It can also check integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithm in network protocols and network applications.

VII. REFERENCES

[1]. Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network,

[2]. Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. 3Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. "A. Handbook of Applied Cryptography". ISBN 0-8493-8523-7.

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

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

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

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

[7]. 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.
[8]. Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644-654.
[9]. Koblitz, N., 1987. “Elliptic curve cryptosystems. Mathematics of Computation” 48, 203-209.
[10]. M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen, M. Schl□a er, \Rebound distinguishers: results on the full Whirlpool compression function," Advances in Cryptology, Proceedings Asiacrypt'09, LNCS 5912, M. Matsui, Ed., Springer, Heidelberg, 2009, pp. 126-143.
[11]. NIST Special Publication 800-38B, “Recommendation for Block Cipher Modes of Operation”: The CMAC Mode for Authentication, May 2005.