Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-1 Issue-1, May 2021

Cryptography in Cloud Computing

Harjinder Kaur, Amandeep Kaur

Abstract: ***Cryptography is a key element in establishing trust and enabling services in the digital world. It is represented in a ways that are not accessible to human users. Hence, humans are left out the trust and security in the digital world. Cryptography is necessary in modern communication protocols and to many digital services. A primitive or protocol should be defined to reach the security goal. Beside the introduction part this paper represents the types of cryptography, algorithm of cryptography and techniques of cryptography and the interaction between Government and cryptography.***

Keyword: Cryptography, Algorithms, Techniques, Symmetric, Asymmetric.

I. INTRODUCTION

Cryptography in the cloud computing defines the encryption techniques to secure the stored data at cloud [1]. The data that is provided by the cloud through cloud services is protected with encryption. There is a need to provide security against un-trusted cloud operators, which causes a challenge for companies and organizations to store sensitive, confidential information like medical records, financial records or high impact business data. Cryptography increases the privacy of related companies by combination of cloud computing [2]. It provides the safe and secure storage. Cryptography stores the data by converting it into non-readable form. It is a useful technique to solve the various problems that are facing in cloud computing such as security, backup data, network traffic, file storage system, security of host etc. Moreover, encryption prevents utilizes like man-in-the-middle, spoofed attacks and session hijacking.

Cryptography is basically used for the secure communication to developing and analyzing protocols that stop the access of information being shared between the two networks by third parties[3]., An adversary in cryptograph is refer to retrieve the confidential information or data that are secured under various principals of information security. Main principals of cryptography are data confidentiality, authentication and non-repudiation. Consider about two parties A and B. Now A wants to send a message “Message” to B via a secure channel. The message is in the form of plain text that is converted into unreadable form, for this purpose a key is used. After using the key the text is called cipher text and also an encryption process. At the time of receiving, the cipher text is again converted into plaintext by using same key and is called the decryption.

Manuscript received on April 12, 2021.
Revised Manuscript received on May 01, 2021.
Manuscript published on May 10, 2021.
* Correspondence Author
Dr. Harjinder Kaur*, Principal at Akal Group of Technical & Management Institutions, Mastuana Sahib
Prof. Amandeep Kaur, Associate Professor at Akal College of Pharmacy & Technical Education, Mastuana Sahib

II. TYPES OF CRYPTOGRAPHY

- Symmetric Cryptography:- In symmetric cryptography both the enciphering and deciphering keys are identical or some time both are related to each other [4] . Both the keys should be kept more secure otherwise in future secure communication will not be possible. Keys should be more secure and it should be exchanged in a secure channel between two users. Data Encryption Standard(DES) is example of symmetric cryptosystem. By using a single key it works for both encryption and decryption [2]. It ensures authentication and authorization by only one key. It works with high speed encryption as a secret key. It further divided into block cipher and system cipher. In block cipher plaintext is accepted as input of fixed size and same size plaintext is obtained as output. In stream cipher one bit is taken as input and obtained as output after encrypted.
- Asymmetric cryptosystem:- It uses two different keys to send and receive the message. It uses public key for encryption and another key for decryption [4]. Suppose two users A and B needs to communicate. A use public key of B’s to encrypt the message. B use private key to decipher the text. It is also called as public key cryptosystem. The receiver has its own decryption key that is referred to as his private key [2]. Receiver also has to generate an encryption key that is referred to as his public key. In asymmetric third party officially declares a particular public key belongs to a specific person.

III. ALGORITHM OF CRYPTOGRAPHY

- Triple DES:- By using this algorithm hackers eventually learned through the data encryption standard(DES) to defeat the relative case [5]. It is the symmetric algorithm. It uses three individual keys of 56 bit each i.e. total 168 bits. Triple DES is beneficial for financial services and other industries by providing a solution of encryption hardware type.
- RSA:- RSA is a public key encryption algorithm that sent encrypting data over the internet [5]. It is asymmetric algorithm. Message has its own public key that encrypt the message and a private key that decrypt the message. It provides the encryption result as a huge batch that takes a quite bit time for attackers and processing power to break.
- Blowfish:- Blowfish is a symmetric 64 bit algorithm that encrypts the block of message individually [5]. It has featured like tremendous speed and effectiveness. Moreover, it provides the advantage of free availability in the public domain. Its main function is to protect the password.

- Twofish:- Twofish keys used 256 bits in the algorithm [5]. It is the symmetric algorithm. It has only one key. It is very fastest in speed and ideal in nature for hardware and software environment. It can be freely accessible by everyone who wants to use it. Hence, bundled of encryption program need to be used the twofish algorithm.
- AES:- Advanced Encryption Standard (AES) is trusted by U.S. Government and various organizations[5]. It is efficient with 128 bits but it also purposes the 192 and 256 keys. AES is impervious to all attacks. All is the combination of 128,192 or 256 bit cipher.

IV. CRYPTOGRAPHY TECHNIQUES

- Lattice – based cryptography
- Multivariate- based cryptography
- Hash-based signature
- Code based cryptography
- Lattice-based cryptography : It is public key based cryptography that overcomes the RSA from its weakness [6]. It provides multiplying matrices instead of multiplying primes. Its constructions are defined via hardness of lattice problems. For example to obtain the output of nonzero vector an arbitrary basis a lattice is used as input.
- Multivariate-based cryptography : In multivariate, public key scheme feces the difficulty over finite fields to solving systems [6]. It is a complex equation. It is used for both encryption and digital signature. Various asymmetric public keys are developed for encryption schemes, these are low rank and insecure. Hence, there is a need of a scheme that eliminates all the deficiencies of previous ones.
- Hash-based signature : Lamport signature scheme invented in 1979 by Leslie Lamport [6]. For 128 bit security level required a secure hash function that occupies orbitary length input and gives the output of 256 bit length.
  - Private Key: Through private key a random number generator is used to generate the 156 pairs of random number of 256 bits. It produces 2x256x256=16 KB.
  - Public Key: All private key numbers are hashed different by creating 512 different hashes of 256 bit each length. For example if there is a hashed message in depending on its value 0 and 1 , it must choose one number from each pair that comprise the private key. It has sequence of 256 numbers. This sequential number is digital signature that published with plain text message.
- Code-based cryptography : It is used to make the error correcting codes [6]. The algorithms are based on the difficulty of decoding linear codes and are considered robust to quantum attacks when the key sizes are increased by the factor of 4.

V. CONCLUSION

Although there has been some increase in security cloud computing world, no straight solution under applied cryptographic implementation. A shared of ownership between cryptographic algorithm and security policy might be collaborative approach for cloud computing. This paper describes how cryptography involves in human life as security basis. Further its types, algorithm and techniques show the different configuration and task.

REFERENCES

1. www.digitalguardian.com
2. Rishav Chatterjee, Sharmistha Roy, “Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud”, International Journal of Engineering Science and Computing, Volume 7 Issue No. 5, ISSN 2321
3. www.greeksofgreeks.com
4. Sujatha K.,D. Ramya Devi, Kala Rathinam D., “A Review Paper on Cryptography and Network Security ”, International Journal of Pure and Applied Mathematics, Volume 119 No. 17, 2018, 1279-1284, ISSN-1314-3395
5. www.blog.storagecraft.com
6. Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Josang, “The Impact of Quantum Computing on Present Cryptography”, International Journal of Advanced Computer Science and Application, Vol. 9 No. 3, 2018