A REVIEW ON CRYPTOGRAPHY TECHNIQUES USING IN CLOUD ENVIRONMENT

Shaffy Bansal[1], Dr. Vijay Bhardwaj[2]

[1]Research scholar, computer applications, Guru Kashi University, Talwandi Sabo

[2]Asst. Prof. of Dept. of Computer Applications, Guru Kashi University, Talwandi Sabo

ABSTRACT

Data security has become crucial aspect nowadays in every sector. So in order to protect various methods and algorithms have been implemented. It protects its privacy and integrity. In this paper, I have reviewed the cryptography algorithms like Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Cryptography is a process that converts data into a format that is unreadable for unauthorized person. It is a Greek word, means that "Secret Writing". Cryptography is an art or science for achieving security by encodes the readable data into non readable data. This paper is dividing into four sections. In the first section, I am presenting just basic introduction about information security using cryptography. In second section, I am presenting literature review. In third section, I am presenting description about cryptography algorithms like symmetric key algorithms AES, DES. In the third section, I am presenting conclusion and references.

Keywords: *Encryption, Decryption, Cryptography algorithms and Cryptography.*

Abbreviations: AES, DES.

I. INTRODUCTION

Cloud means common location independent online utility on demand. Today it has been made possible that people are consulting their mail online through webmail clients, working on collaborative documents using web browsers and creating virtual albums. People are running applications on servers and even storing their crucial data on servers rather than on their systems. All this has been made possible because of cloud computing Cloud computing is a pay-per-use-on-demand mode that can access shared IT resources through the internet. Cloud computing is the delivery of computing services- storage, servers, databases etc. Suppose two friends who share critical secret information have to split up. Now the problem that arises is that they have to communicate with each other from far of a distance. This distance invites eavesdropper to stop, intercept or interfere the communication between two friends in order to gain access to secret information. So, to avoid this, both the friends decided to lock their secret information in a box and the key to unlocking that box is known only to them. So, when first friend the locked box to the second, he/she unlocks it using the secure combination key Cryptography is the study of information hiding and verification. People who study or develop cryptography are called cryptographers. Cryptography involves the process of Encryption and Decryption.

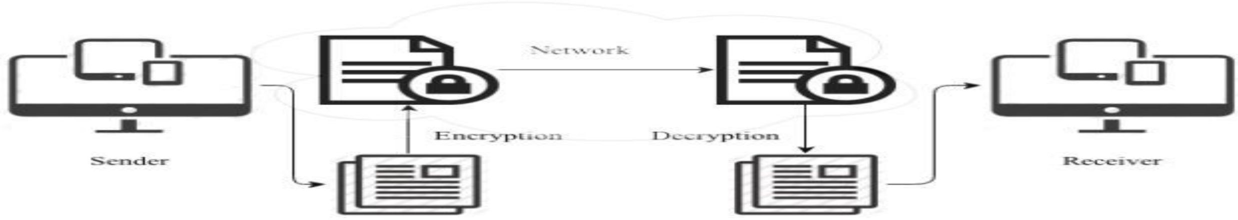


Fig. 1. Cryptography

The various terms which are used in cryptography is given below:

1. Plaintext: The original message which is transmitted to the destination
2. Cipher text: The plain text is converted into readable form.
3. Encryption: The process of converting the readable data into non readable data.
4. Decryption: The reverse process of converting cipher text back into the plain text.
5. Key: It is a value that is used to encrypt the plain text or decrypt the cipher text.

II. LITERATURE REVIEW

Bhardwaj A., Subramanian GVB. et al., 2016, stated that with growing awareness and concerns regards to Cloud Computing and Information Security, there is growing awareness and usage of Security Algorithms into data systems and processes. In this paper we review

Symmetric and Asymmetric algorithms with emphasis on Symmetric Algorithms for security consideration on which one should be used for Cloud based applications and services that require data and link encryption. With Cloud computing emerging as a new in thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. This makes Cloud security a must to break the acceptance hindrance of the cloud environment. Use of security algorithms and ensuring these are implemented for cloud and needs to be properly utilized in order to ensure end user security. [1]

Vurukonda N., Thirumala Rao B., 2016, stated that cloud computing is a revolutionary mechanism that changing way to enterprise hardware and software design and procurements. Because of cloud simplicity everyone is moving data and application software to cloud data centers. The Cloud service provider (CSP) should ensure integrity, availability, privacy and confidentiality. [2]

Khan S.S., Tuteja R.R., 2015, stated that cloud computing is a set of IT Services, for example network, software system, storage, hardware, software, and resources and these services are provided to a customer over a network. The IT services of cloud computing are delivered by third party provider who owns the infrastructure. So there is a need to protect that data against unauthorized access, modification or denial of services etc. To secure the Cloud means secure the treatments (calculations) and storage (databases hosted by the Cloud provider). In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers. [3]

Patil P. et al. , 2015, explains that in today's internet era, with online transactions almost every second and terabytes of data being generated everyday on the internet, securing information is a challenge. Cryptography is an integral part of modern world information security making the virtual world a safer place. Cryptography is a process of making information unintelligible to an unauthorized person. Hence, providing confidentiality to genuine users. There are various cryptographic algorithms that can be used. Ideally, a user needs a cryptographic algorithm which is of low cost and high performance. [4]

III. CRYPTOGRAPHY ALGORITHMS

The Cryptography algorithms are grouped into two categories:

Symmetric key cryptography and Asymmetric key cryptography.

Symmetric key cryptography is used only one key for encryption or description. The key is said to be private key. It is also called as single key cryptography. Symmetric key algorithms are those in which sender and receiver are use the same key.

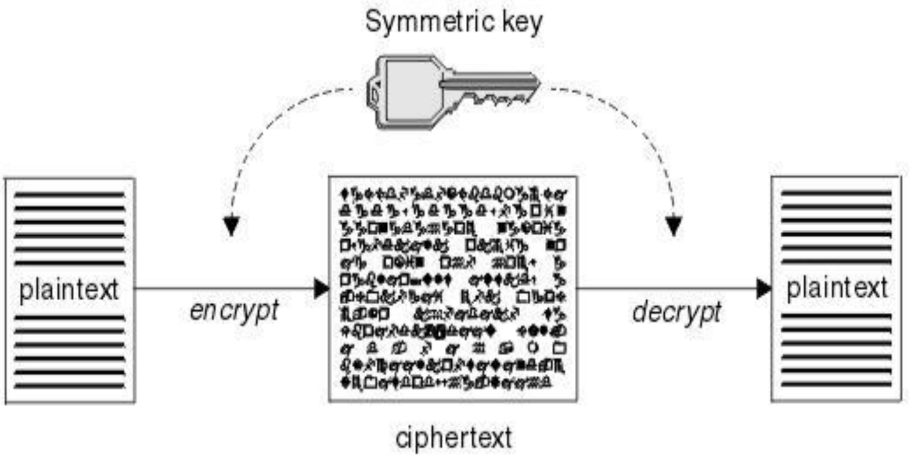


Fig. 2. Symmetric key algorithm

Examples of single key algorithm are as follows:

1. Data Encryption Standard (DES)
2. Advanced Encryption Standard (AES)

Data Encryption Standard: It is a symmetric key block cipher published by the National Institute of Standards and technology. It is developed in 1970s and it uses 16 round feistel structure. It has 64 bit block size and key size is 64 bit but DES has an effective key length of 56 bits, since 8 0f the 64 bits of the key are not used by the encryption algorithm. DES uses the same key for encryption and decryption.

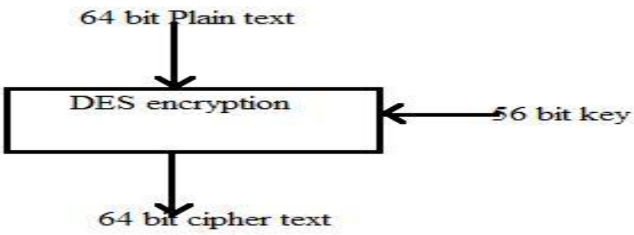
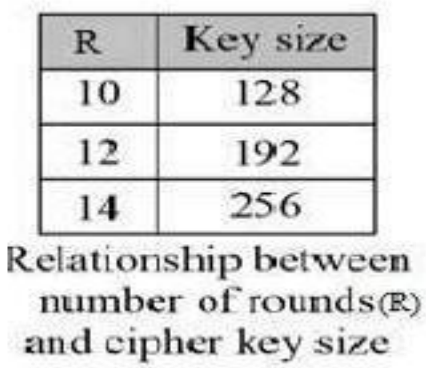


Fig. 3. Basic structure of DES

Advanced Encryption Algorithm: It is a symmetric key encryption standard adopted by the in US government in 2001. It was designed by Vincent Rijmen and Joan Daemena in 1998 later inspected by National Institute of Standards and Technology (NIST) as U.S. FIPS in November, 2001. It has 128 bits block size and 128, 192, 256 bits key sizes. The number of rounds are not fixed in AES depends on the key size. 128 bits key require 10 rounds and 192 bits key require 12 rounds and 256 bits key require 14 rounds.

Table 1 AES Versions



R	Key size
10	128
12	192
14	256

Relationship between
number of rounds(R)
and cipher key size

Asymmetric key cryptography is used two for encryption that is one key is to encrypt the plaintext and other key is used to decrypt the cipher text.

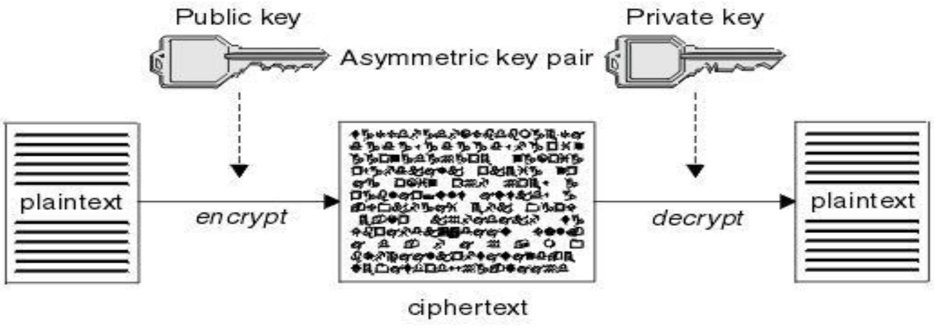


Fig. 4. Asymmetric key algorithm

IV. CONCLUSION

Cloud Computing can become more secure using cryptographic algorithms. Cryptography is the art or science of keeping messages secure by converting the data into non readable forms. But the existing cryptographic algorithms are single level encryption algorithms. Cyber criminals can easily crack single level encryption. Hence we propose a system which uses multilevel encryption and decryption to provide more security for Cloud Storage.

REFERENCES

[1] Preetha M., Nithya M., "A study and performance of RSA algorithm*", International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 2, Issue. 6, June 2013, pg.126 – 139.

[2] Kumar Y., Munjal R. et al. "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures"**,** *IJAFRC*, Volume 1, Issue 6, June 2014.

[3] Pahal R., Kumar V., "Efficient Implementation of AES", IJARCSSE, Volume 3, Issue 7,July 2013.

[4] Aggarwal A., Singh G. et al., " Implementation of AES algorithm", *International Journal of Engineering Research & Science (IJOER)*, Vol-2, Issue-4 April- 2016, pp. 112-116.

[5] Bhardwaj A., Subrahmanyam GVB. et al., "Security Algorithms for cloud computing",*International Conference on Computational Modeling and Security, Procedia Computer Science 2016*, pp. 535 – 542.

[6] Vurukonda N., Thirumala Rao B., "A Study on Data Storage Security Issues in Cloud Computing", *2nd International Conference on Intelligent Computing, Communication & Convergence, Procedia Computer Science 92*, 2016, pp. 128 – 135.

[7] Khan S.S., Tuteja R.R., "Security in Cloud Computing using Cryptographic Algorithms", *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)*, Vol. 3, Issue 1, January 2015, pp. 148 – 154.

[8] Patil P. et al., "A comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish", *International Conference on Information Security & Privacy (ICISP2015),* Nagpur, 11-12 December 2015, Volume 78, 2016, pp. 617-624.

[9] Mohd. A. et al., "AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation", *7th International Conference on Information Assurance and Security, IAS 2011*, Melacca, Malaysia, December 5-8, 2011, pp. 292 – 297.

[10] Abhilasha CP et al., "Software Implementation of AES Encryption Algorithm", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, Volume 6, Issue 5, May 2016, pp. 201 - 205 .

[11] Meena M.et al., "A study and comparative analysis of cryptographic algorithms for various file formats", *International Journal of Science and Research (IJSR)*, 2013, pp. 991 - 995.

[12] Shakeeba et al., "Cloud Security using Multilevel Encryption Algorithms", *International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE)*, Vol. 5, Issue 1, January 2016, pp. 70 – 75.