DESCRIPTIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS FOR SECURING CLOUD COMPUTING.

Akansha singh
Dept. Of Computer Science and Engineering, Goel Institute of Technology and Management
Dr. APJ Abdul Kalam University, Lucknow, India

Abstract: Cloud computing is one of the most promising technology being used by numerous organizations at present. Organizations are accepting cloud for its entire requirements related to platform, storage or infrastructure. But the major concern of any organization is assurance from security breaches and cyber-attacks.
There exist many means to store the data onto the cloud with maximum protection from unauthorized intruders. One of the basic yet promising means is cryptography. This paper has description of all the ciphers and cryptographic algorithms that can be used for data protection on cloud.
This paper is suggested suitable for beginners in research in cloud security by cryptographic algorithms for security of data over cloud.

Index Terms **- Cloud computing, encryption, decryption, DES, 3DES, AES, BOWFISH.**

I. INTRODUCTION

Data is one of the most crucial resources of any organization. The management of data in its own infrastructure is very difficult now days as humongous amount of data is generated each day, where every information is important for future decision making and organizational growth.
To overcome this issue cloud computing was introduced were any organization can hire online storage, infrastructure, software etc as per its requirement and pay for only those services which are used by the organization. The cloud service providers provide all the services desired by the organization. Cloud computing is an evolving technology that has changes the way IT architectural solutions were found. It is a new pattern of business computing, and it can dynamically provide computing services such as infrastructure, memory, OS, etc. [5]
According to NIST (national institute of standards and technology) ," *cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources(e.g. network , serves , storage, application and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[1]*
But one of the most critical issues in cloud computing is security. With the advancement of the Internet and Web technology, it is necessary for people to be able to access and manage information from any location in most efficient manner. Cloud computing provides information resources to users in "Cloud" through the Internet at any location and by using any computing device. Cloud computing utilizes large-scale virtualized resources to manage such large volume of data. [6]
The cloud provider has all the crucial data of any individual or organization and can easily misuse the confidential data. Security breach can be done at providers end and also between the networking medium.

II. PROBLEM ANALYSIS

From the last few years, there has been a high advancement in Cloud Computing. Cloud Computing provides a wide range of resources like computational power, platforms, storage area and applications that can be easily used over internet. Some major challenges that are being faced by Cloud are to secure from intruders so that processing of the data is done only by authorized user. Below are the two main states that have chances of unauthorized access to the data: when the data is in motion (transit) and when the data is at rest, where the data is much expected to be more secure. The below illustrated are the two main scenarios which we have focused to understand the security of the data in the Cloud. [11]

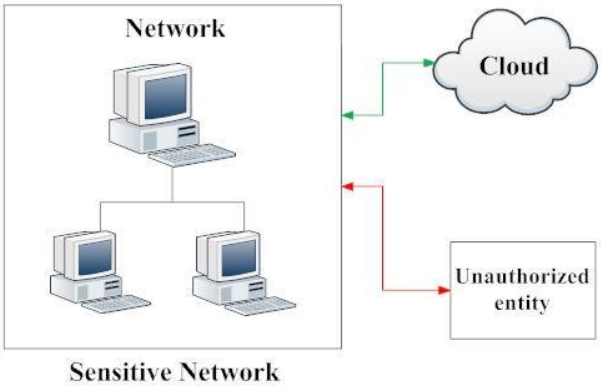


Fig 1: unauthorized access of data from network.

The above figure 1 describes a scenario where a local network is connected to a Cloud network, in which some part of the network data is broken out from the local network and placed in the Cloud, but the critical data resides in the local network itself. In this case, the Cloud provider does not have any authority of accessing the data physically which is in the local network. But for instance, the Cloud needs to access some information which is in the local network, during that access; there exists a possibility of unauthorized access of the local network resources. It explains the typical problem in network security where the information can face both active attacks and passive attacks. These attacks are likely to happen when the block of information leaves the client network to the Cloud network.

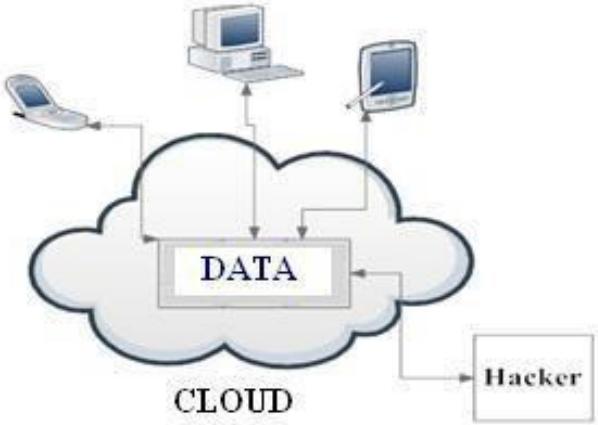


Fig 2: unauthorized access of data from cloud.

The above figure 2 describes the scene where the total data of the local network is placed within the Cloud, where the local network and the authorized users both have privilege to access the data physically present in the Cloud. At that particular time, here exists a possibility for unauthorized users to enter the cloud and access the confidential data in the Cloud. In this situation, the virtual machines are allotted to authorized users of the Cloud. These machines have valid logins. However, these logins can be cracked. The data may also be accessed in other ways too. Regarding this aspect of data loss, most of the research papers followed a normal traditional literature survey method.

III. CRYPTOGRAPHY

In this era of global electronic connectivity, viruses and hackers, electronic eavesdropping and electronic fraud, there is indeed no time at which security is not a major concern.[4] In context of cloud computing security of data being uploaded onto the cloud is the major concern of the cloud user. Cryptography can reformat and transform our data, making it safer on its trip between source and cloud.

Cryptographic algorithms are used for ensuring privacy, authenticity and secrecy of confidential data or information. Cryptography uses mathematical functions and operations for encryption and decryption of data.

We can define cryptography as, **"The art and science encompassing tools and techniques to convert confidential meaningful message/text into meaningless message/text."[4]**

Some basics terminologies of cryptography are as follows:

1. **Plain text:** The meaningful message/text that is to be converted into cipher text.

2. **Cipher text:** The meaningless message/text produced as output after encryption of plain text.

3. **Key:** The critical set of information that is known by sender and receiver and is used for both encryption and decryption.
4. **Cipher:** The algorithm or tool used for converting plain text into cipher text.
5. **Encryption:** The process of converting plain text into cipher text.
6. **Decryption:** The process of converting cipher text into plain text.
7. **Cryptanalysis:** The study of principle and methods of encryption and decryption without the prior knowledge of key is called cryptanalysis, also known as code breaking.

3.1. CLASSIFICATION OF CRYPTOGRAPHIC ALGORITHMS

The fundamental task of cryptography is to convert plain text into cipher text using keys. Performance evaluation of cryptographic algorithms is done by following factors which are:

- Encryption time
- Decryption time
- Memory usage
- Flexibility
- Scalability
- Security

Ciphers can be classified into basic two types.

1. Classic cryptographic ciphers:

These are further classified into two variants.

1.1. Substitution cipher:

In this cryptographic algorithm, each unit of plain text is replaced using the key for converting plain text into cipher text. It is fundamental cipher and very easy to decode.

1.2. Transposition ciphers:

In cryptography, transposition cipher is encryption method where the units of plain text are shifted by positions as per the key being used.

2. Modern cryptographic algorithms:

The present era has high security threats. It is very difficult to secure data from external as well as internal security attacks and breaches. Ciphers can be further classified into two types:

2.1. Symmetric key algorithm:

In cryptography, symmetric key algorithms are the one which uses same key for both encryption as well as decryption. These algorithms share the secret key only between the sender and receiver. Both sender and receiver have prior knowledge of the secret key and is in case any unauthorized third party gains access to the key then it is very easy for him to crack the code and decrypt the confidential message/text.

2.2. Asymmetric key algorithms:

Asymmetric algorithms are the one which uses different key for encryption and decryption of the message /text. In such algorithms the key used for encryption is completely different from the key used for decryption. The key being used for encryption is public key and is broadcasted amongst all the senders but the decryption of data is done through private key known only by the receiver.

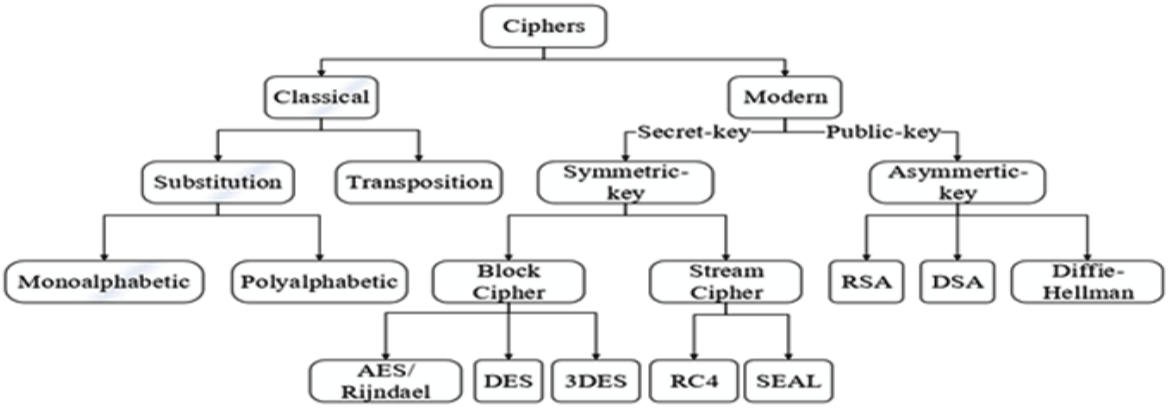
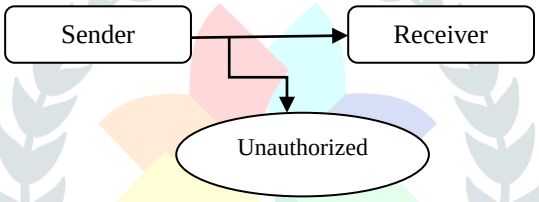


Fig 3: Classification of cryptographic algorithms. [10]

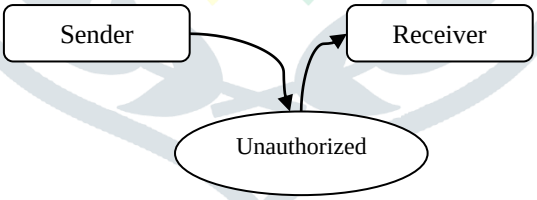
IV. SECURITY ATTACKS:

There are basically four categories of security attack, which are as follows:

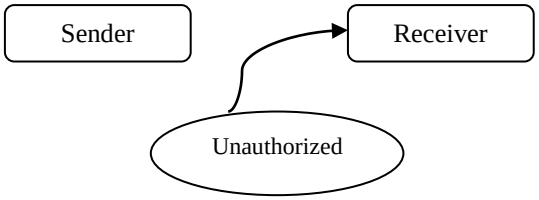
1. Interruption: It refers to the process of interrupting between the sender and receiver, for instance destroying the channel of communication or damaging the hardware etc.
2. Interception: When an unauthorized third party gains access to the network and eardrops the confidential information.



3. Modification: The unauthorized third party tampers with the original message or text and sends the modified text to the authorized receiver.



4. Fabrication: An unauthorized party adds fake or self-generated text to the medium after gaining access.



V. OVERVIEW OF SYMMETRIC CRYPTOGRAPHIC ALGORITHMS

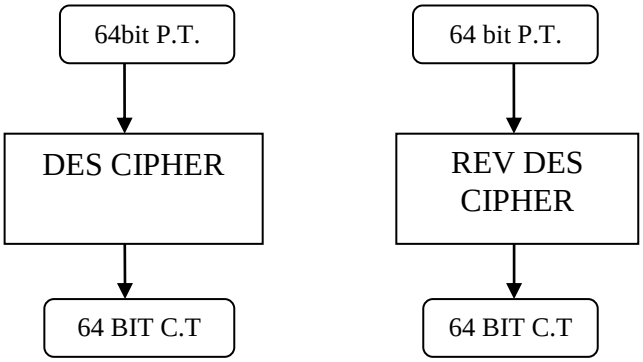
5.1. DATA ENCRYPTION STANDARD (DES)

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). [3]It was developed by IBM in 1970 but was later accepted by NIST.

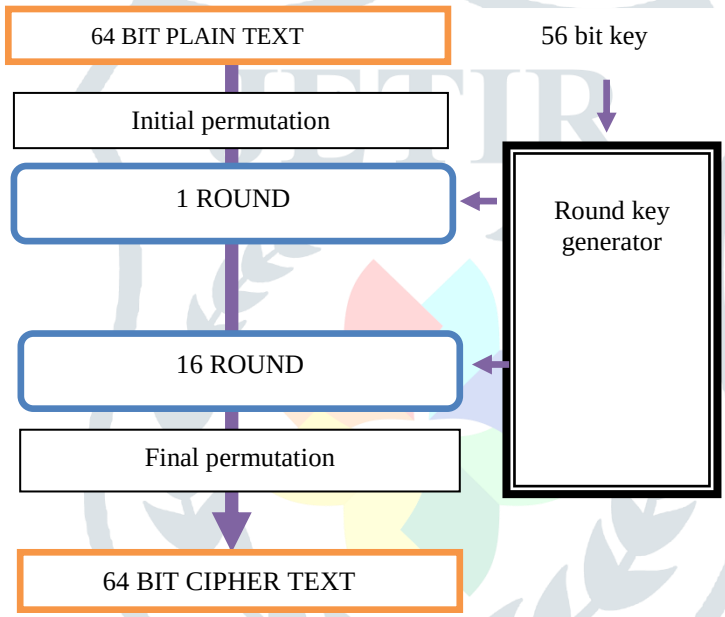
5.1.1.Characteristics of DES:

i. Symmetric key cipher

ii. The encryption process is done block wise.
iii. Converts 64 bit P.T. text into 64 bit C.T.
iv. It uses 56 bit key.



5.1.2. General structure of DES:



5.1.3. DES Analysis:

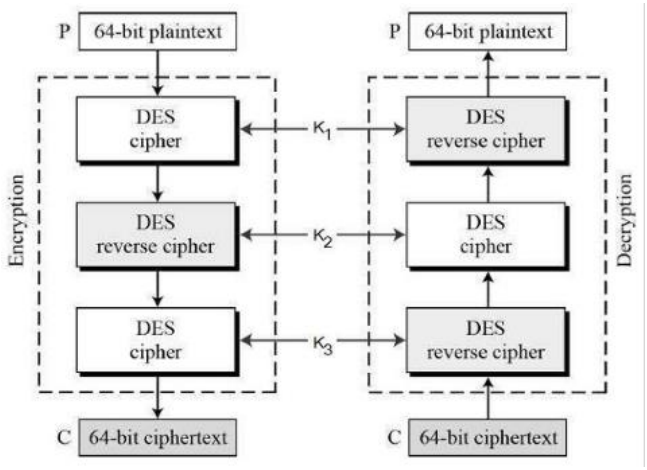
The two properties that make DES cipher very strong are:
Avalanche effect: A small change in plaintext results in the very great change in the cipher text, i.e. if any single bit of plaintext is changed then many bits of must be changed.
Completeness: Each bit of cipher text depends on many bits of plaintext, i.e. a single bit of cipher text is result of encryption done at many bits of plaintext.

5.2. TRIPLE – DES (3DES)

DES is widely used encryption algorithm but since 1990 it was difficult to secure data from cryptanalysis due to small key size. 3DES is designed to overcome obvious flaws of DES without introducing a totally new cryptographic algorithm. [3]
There exist two different variants of 3DES they are:

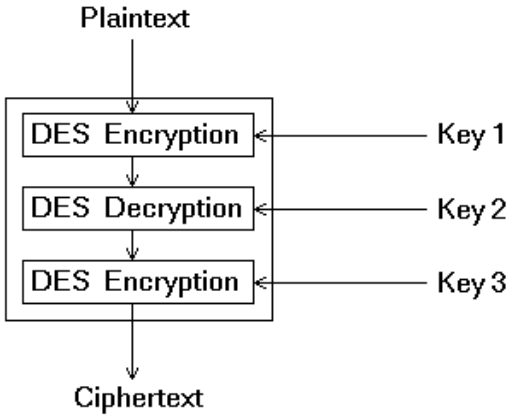
5.2.1. 3DES using 3 keys:

Here 3 different keys are used namely k1, k2, k3 for each step in 3 DES.



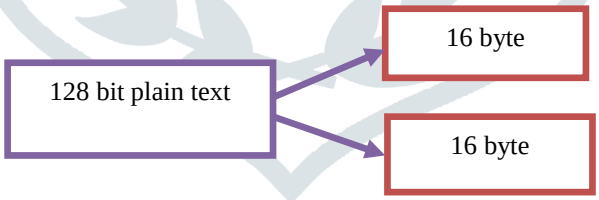
5.2.2. 3DES using 2 keys:

Here 2 different keys are used namely k1, k2 for each step in 3 DES.



5.3. ADVANCED ENCRYPTION STANDARDS (AES)

Advanced encryption standards (AES) is the most widely used cipher. The biggest limitation of DES was small key size which is resolved by AES; also AES is 6 times faster than 3DES algorithm both in terms of encryption and decryption. [2][7]

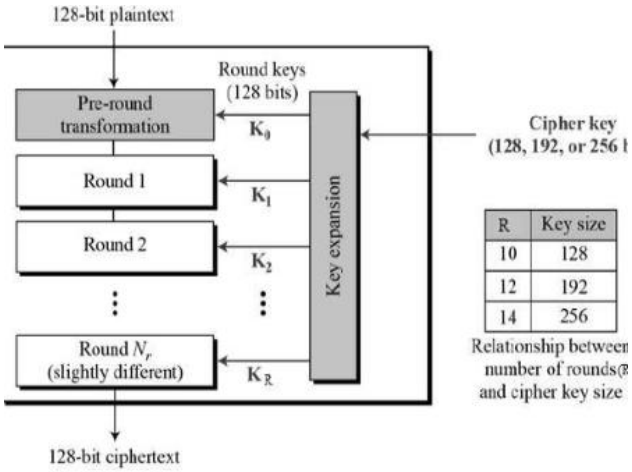


5.3.1. Characteristics of AES:

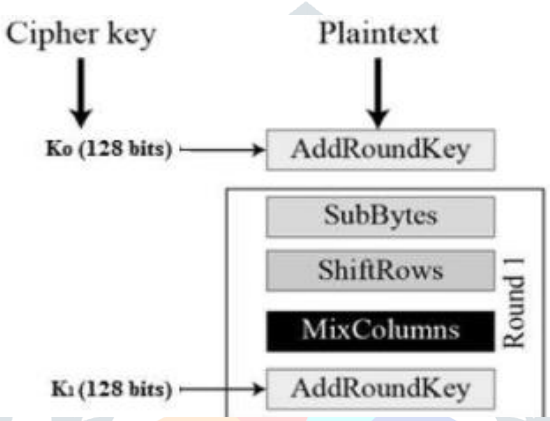
Some basic features of AES are as follows:

- Symmetric key cipher
- 128 bit data
- Stronger and faster than DES.

5.3.2. Basic structure of AES:



5.3.3. Encryption process of AES:



5.3.4. AES Analysis:

AES is the most promising encryption algorithm being used for cloud computing security. AES is a strong and best among all the symmetric algorithms in terms of encryption time, decryption time, flexibility etc. [2][9]

5.4. BLOWFISH ALGORITHM

Blowfish Algorithm was developed by Bruce Schneier in 1993 it is a symmetric block cipher i.e. it converts block of plain text into cipher text using same key for both encryption and decryption. [8]

5.4.1. Characteristics of blowfish algorithm:

- Some properties of blowfish algorithm are as follows:
- It is very fast algorithm.
- It easily executes on very less memory space.
- It uses simple XOR operations for encryption and decryption of data.
- Highly secure due to variable length of key.

Blowfish algorithm encrypts 64 bit of plain text into 64 bit of cipher text using variable length of key ranging from 32-448bits.

5.5. RSA

It was invented by three scholars Ron Rivest, Adi Shamir, and Len Adleman and therefore, it is termed as RSA cryptosystem. RSA is a public key cryptographic cipher. Unlike symmetric key, public key ciphers have 2 different keys for encryption and decryption of data.

5.5.1. Implementation of RSA:

- Choose any two prime no.'s P and Q such that P is not equal to Q.
- Calculate N = P * Q
- Choose E (public key) such that E is not a factor of (P-1) and (Q-1).

- Choose D such that (D*E) mod (P-1)(Q-1) = 1.
- CIPHER TEXT = $(P.T)^{E}$ mod N
- PLAIN TEXT = $(C.T.)^{D}$ mod N

VI. CONCLUSION AND FUTURE WORK

This paper presented a detailed study of all the cryptographic algorithms present in market currently for encryption of data being uploaded on cloud. It is seen that all the algorithms have their own characteristics and methodology for encrypting plain text into cipher text. According to the work done and literature survey it can be induced that AES is one of the most promising algorithm for security of data stored at cloud.
In order to ensure the same, the performance matrix must be maintained and each parameter must be checked in order to verify which algorithm can be suitable as per the requirement.
Our future work will be on implementation of all these algorithm individually and also combination of two or more algorithm in order to generate more promising and secure environment for data storage and retrieval from cloud. [3]

VII. COMPARATIVE STUDY OF SECURITY ALGORITHM

Factors	DES	3DES	BLOWFISH	AES	RSA
CREATED BY	IBM in 1975	IBM in 1978	Bruce Schneier in 1993	Vincent Rijmen in 2001	Ron Rivest, Adi Shamir, and Len Adleman in 1978
KEY LENGTH	56 bit	128 bit	32-448 bit	128,192 or 256 bit	Depends on no f bits in modulus n
NO. OF ROUNDS	16	48	Variable (till all the P and S boxes are replaced)	10, 12 or 14	1
BLOCK SIZE	64 bit	64 bit	64 bit	128 bit	variable
CIPHER TYPE	Symmetric cipher	Symmetric cipher	Symmetric cipher	Symmetric cipher	Asymmetric cipher

REFERENCES

1. Akansha singh, “Cloud computing: A brief descriptive review along with its security issues and challenges”, IEEE International conference (IJAER) volume 14, number 2, Feb-2019.
2. Abdul raoof wani, Q.P.Rana, “Performance Evaluation And analysis Of Advanced Symmetric Key Cryptographic Algorithms For Cloud Computing Security”, Springer nature Singapore pte ltd. ,2019.
3. Gurpreet singh, “A study of encryption algorithms (RSA, DES, 3DES and AES) for information security”, IJCA, 2013.
4. William Stallings “Cryptography and Network Security_ Principles and Practice”, pp. 1-20.
5. Meyer, C.H.: Cryptography-a state of the art review. In: omp Euro’89., VLSI and Computer Peripherals. VLSI and Microelectronic Applications in Intelligent Peripherals and their Interconnection Networks’, Proceedings. IEEE (1989).
6. Krutz, R.L., Dean Vines, R.: Cloud Security: Comprehensive Guide to Secure Cloud Computing. Wiley Publishing (2010).
7. Priyansha Garg, Moolchand Sharma, Shivani Agrawal and Yastika Kumar,“Security on Cloud Computing Using Split Algorithm Along with Cryptography and Steganography”, International Conference on Innovative Computing and Communications.

8. SuvenduKuila, ShruthiShridhar, Chandan Patel and N. Ch. S.N Iyengar, "Cloud Computing Security by Using Mobile OTP and an Encryption Algorithm for Hospital Management" Journal of Computer and Mathematical Sciences, Vol.7(11), 558-565, November 2016 ISSN 0976-5727.
9. Vishal R. Pancholi, Dr.Bhadresh P. Patel, "Enhancement of Cloud Computing Security with Secure Data Storage using AES" IJIRST –International Journal for Innovative Research in Science & Technology| Volume 2 | Issue 09 | February 2016 ISSN (online): 2349-6010
10. Joseph Selvanayagam1, Akash Singh2, Joans Michael3, Jaya Jeswani4 "SECURE FILE STORAGE ON CLOUD USING CRYPTOGRAPHY", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 05 Issue: 03 | Mar-2018.
11. Shweta Kaushik "Cloud data security with hybrid symmetric encryption", 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT).