Cloud Computing Security Algorithms Comparative Analysis

[1]T.Kavitha [2] K Siva Rama Krishna, [3] Dr.V.Harsha Shastri
[1, 2, 3]Lecturer in Computer Science, Loyola Academy, Alwal, Secunderabad, TS, India.

Abstract:

Cloud Computing is an emerging technology in today's business era. Cloud computing is a word which describes different computing concepts which contains huge number of computers attached through a real-time communication like internet. Cloud computing is also called distributed computing over the network i.e. the ability to execute an application or a program on many computers at the same time. As many organizations are moving data to the cloud there is a need to protect data against unauthorized access. 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. This paper presents a brief overview and comparison of security algorithms

Keywords: **Cloud Computing, Security, Public Cloud, RSA, Blowfish, RC6.**

I. Introduction

Cryptography [1] can be seen as a method of storing and disguising confidential data in a cryptic form so that only those for whom it is intended can read it and are able to communicate information in the presence of an adversary and the security algorithms mitigate security issues by use of cryptography, authentication and distributing keys securely. Cryptography is thus the science of making data and messages secure by converting the end user data to be sent into cryptic non-readable form and encrypting or scrambling the plaintext by taking user data or that referred to as clear text and converting it into cipher text [2] and then performing decryption which is reverting back to the original plain text. With this ability, Cryptography is used for providing the following security:

- Data Integrity: information has value only if it is correct, this refers to maintaining and assuring the accuracy and consistency of data, its implementation for computer systems that store use data, processes, or retrieve that data.
- Authentication for determining whether someone or something is, in fact, who or what it is declared to be.
- Non Repudiation: is the assurance that a party, contract or someone cannot deny the authenticity of their signature and sending a message that they originated.
- Confidentiality: relates to loss of privacy, unauthorized access to information and identity theft.

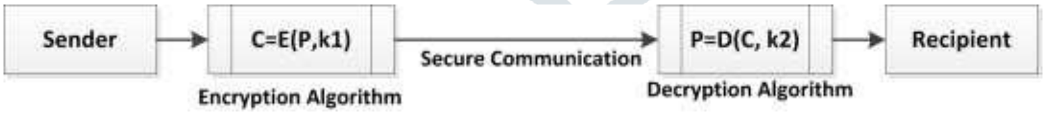

Fig 1: Encryption and Decryption process

In pure science terms [3], Cryptography is the science of using mathematics for making plain text information (P) into an unreadable cipher text (C) format called encryption and reconverting that cipher text back to plain text called as decryption with the set of Cryptographic Algorithms (E) using encryption keys (k1 and k2) and the decryption algorithm (D) that reverses and produces the original plain text back from the cipher text. This can be interpreted as Cipher text C = E {P, Key} and Plain text C = D {C, Key}

Defining some terms used in Cryptography:

- Plaintext is the original intelligible source information or data that is input to algorithms
- Cipher text is the scrambled message output as random stream of unintelligible data
- Encryption Algorithm substitutes and performs permutations on plain text to cipher text
- Decryption Algorithm is encryption run in reverse by taking the secret key and transforming the

cipher text to produce the original plain text

- Keys are used as input for encryption or decryption and determines the transformation
- Sender and Recipients are persons who are communication and sharing the plaintext

With respect to Cloud computing, the security concerns [4] are end user data security, network traffic, file systems, and host machine security which cryptography can resolve to some extent and thus helps organizations in their reluctant acceptance of Cloud Computing. There are various security issues that arise in the Cloud:

- Ensuring Secure Data Transfer: In a Cloud environment, the physical location and reach are not under end user control of where the resources are hosted.
- Ensuring Secure Interface: integrity of information during transfer, storage and retrieval needs to be ensured over the unsecure internet.
- Have Separation of data: privacy issues arise when personal data is accessed by Cloud providers or boundaries between personal and corporate data do not have clearly defined policies.
- Secure Stored Data: question mark on controlling the encryption and decryption by either the end user or the Cloud Service provider.
- User Access Control: for web based transactions (PCI DSS), web data logs need to be provided to compliance auditors and security managers.

II. Security Algorithms

Two techniques in Security algorithms are Symmetric Algorithms and asymmetric Algorithms.

Symmetric algorithms: (also called "secret key") use the same key for both **encryption** and decryption.

Asymmetric algorithms: (also called "public key") use different keys for **encryption** and decryption

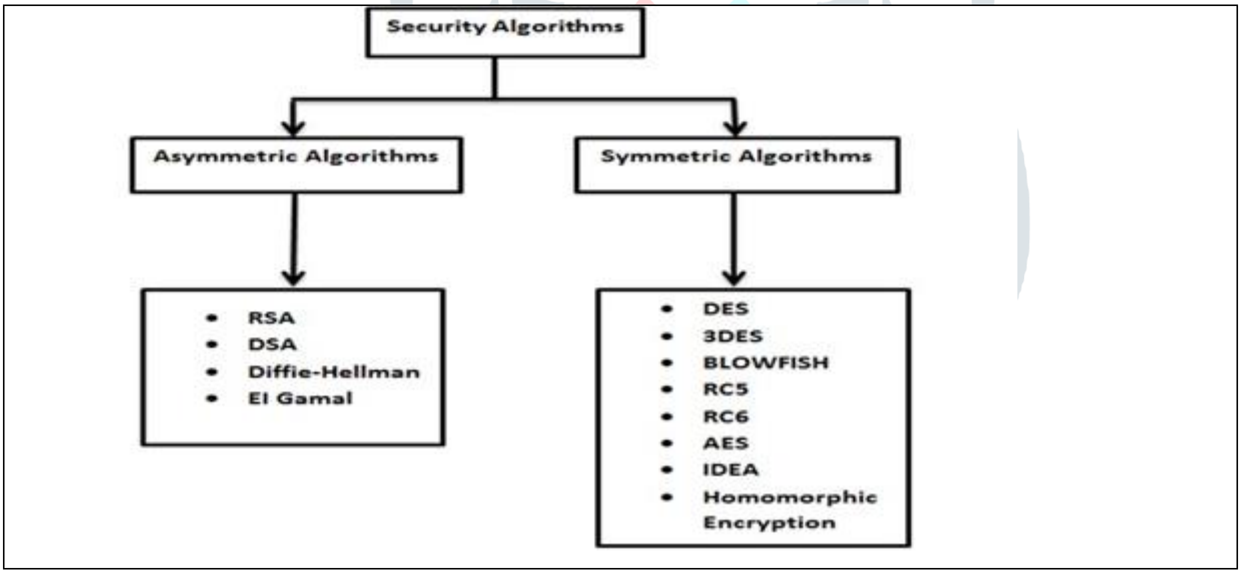

Fig 2: Security Algorithms

A. DES

DES stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher [4].

Algorithm:

```
Function DES_Encrypt (N, K) where M = (L, R) N ←IP(N)
        For round ←1 to 16 do $K_i$ ←SK (K, round) L ←L xor F(R, Ki)
swap(L, R)
        end swap(L, R)
        M ←$IP^{-1}$(N)
return N End
```

B. *BLOWFISH*

Blow fish algorithm was developed in 1993. It is one of the most common algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [5].

Algorithm:

```
Divide x into two 32-bit halves: $x_L$, $x_R$ For i = 1to 16:
        $X_L$= $X_L$XOR $P_i$ $x_R$= F($X_L$) XOR $x_R$

        Swap $X_L$and $x_R$ Next i
        Swap $X_L$and $x_R$(Undo the last swap.) $x_R$= $x_R$XOR $P_{17}$
$x_L$= $x_L$XOR $P_{18}$

Recombine $x_L$and $x_R$
```

C. *RC2*

RC2 is a symmetric block cipher that operates on 64 bit quantities. It uses a variable size key, but 128 bit key would normally be considered good. RC2 can be used in all the modes that DES can be used. A proprietary algorithm developed by RSA Data Security, Inc,. The algorithm expands every single message by up to 8 bytes. RC2 is a block cipher that encrypts data in blocks of 64 bits[6].

D. *RC5*

RC5 was developed in year 1994. The key length if RC5 is MAX2040 bit. The block size of RC5 is 32, 64 or 128. The use ofRC5 algorithm shows that it is Secure. The speed is slow [7].

Algorithm:

```
     C = C + S[0];
     D = D + S[1];
for i = 1 to f do
    C = ((C Xor D) <<< D) + S[ 2 * i ]
    D = ((D Xor C) <for i = 1 to f do Next
```

E. *RC6*

RC6 algorithm has a block size of 128 bits. The key sizes of 128, 192 and 256 bits. RC6 is developed in same structure of RC5, having data-dependent rotations, XOR operation and modular addition. RC6 could be viewed as interweaving two parallel RC5 encryption Techniques. Though, RC6 can use an extra multiplication operation not present in RC5 in order to make the rotation dependent on each bit, and not the least significant few bits[6].

F. *3DES*

3DES was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to theone in original DES but applied three times to increase the encryption level. But 3DES is slower thanother block cipher methods. 3DES is an enhancement of DES and it is 64 bit block size and with 192 bits key size. 3DES requires always moretime than DES because of its triple phase encryption characteristics. 3DES haslow performance in terms of power consumption and throughput when compared with DES[5][8].

Algorithm:

```
For j = 1 to 3
{
$C_{j,0}$= $IV_j$

For i = 1 to $n_j$
{
$C_{j,i}$= $E_{KEY3}$ ($D_{KEY2}$($E_{KEY1}$($P_{j,i}C_{j,i-1}$)))

Output $C_{j,i}$

}
}
```

G.AES

AES stands for Advanced Encryption Standard. It is the new encryption standard recommended by NIST to replace DES. The Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. AES have key length of 128, 192, or 256 bits, by default 256. This can encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. AES has been carefully tested for many security applications[8][9].

Algorithm:

```
Cipher(byte[] input, byte[] output)
    {
byte[4,4] State;
copy input[] into State[] AddRoundKey for (round = 1; round < Nr-1; ++round)
        {
SubBytesShiftRowsMixColumnsAddRoundKey
        }
SubBytesShiftRowsAddRoundKey copy State[] to output[]
    }
```

H. RSA

RSA was an encryption and authentication technique that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the commonly used encryption techniques. Up-to-Date it is the only algorithm used for private and public key generation and encryption. RSA is a fast encryption [14].

Algorithm:

Key Generation: KeyGen(r, s) **Input**: Two large primes – r, s Compute n = r .s
φ (n) = (r - 1)(r - 1)
Choose e such that gcd(e, φ (n)) = 1 Determine d such that e .f ≡ 1 mod φ (n) **Key:**
public key = (e, n) secret key= (f, n) **Encryption:**

$c = m^e \bmod n$
where c is the cipher text and m is the plain text.

RSA has a multiplicative homomorphic property i.e., it is possible to find the product of the plain text by multiplying the cipher texts. The result of the operation will be the cipher text of the product.
Given $c_i = E(m_i) = m_i^e \bmod n$, then
$\mathbf{(c1\ .\ c2)\ mod\ n = (m1\ .\ m2)^e\ mod\ n}$

I. DSA

DSA stands for Digital Signature Algorithm which was proposed by the NIST in August 1991 for use in their DSS and adopted as FIPS 186 in 1993. The four revisions to the initial specification have released. In DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical. DSA is so critical that violating any one of those three requirements can reveal the entire private key to the third party. Using the same value twice, using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA [9].

J. DIFFIE-HELLMAN Key Exchange

Diffie–Hellman key exchange was a specific method of exchanging cryptographic keys. The D-H key Exchange is one of the earliest practical examples of key exchange implemented within the field of cryptography. The D–H key exchange method allows two users that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. In this, the key can then be used to encrypt subsequent communications using a symmetric key cipher [10].

K. *TWOFISH*

Bruce Schneier is the person who composed Blowfish and its successor two fish. The Keys used in this algorithm may be up to 256 bits in length .Two fish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Two fish is also freely available to anyone who wants to use it. As a result, we'll find it bundled in encryption programs such as Photo Encrypt, GPG, and the popular open source software True Crypt[11].

L. *IDEA*

IDEA stands for International Data Encryption Algorithm which was proposed by James Massey and Xuejia Lai in 1991. IDEA is considered as best symmetric key algorithm. It accepts 64 bits plain text. The key size is 128 bits. IDEA consists of 8.5 rounds. In IDEA the 64 bits of data is divided into 4 blocks each having size 16 bits. The basic operations are modular, addition, multiplication, and bitwise exclusive OR (XOR) are applied on sub blocks. There are eight and half rounds in IDEA each round consist of different sub keys. Maximum number of keys used for performing different rounds is 52 [12].

M. *EIGAMAL*

The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the D–H key exchange. EIGamal was described by Taher Elgamalin 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The DSA is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. The security of EIGamal depends on the difficulty of a particular problem in related to computing discrete logarithms [13].

N. *HOMOMORPHIC ENCRYPTION*

Homomorphic encryption was a one of encryption technique which allows specific types of computations to be carried out on cipher text. It gives an encrypted result which when decrypted matches the result of operations performed on the plaintext. When the data is transferred to the cloud we use standard encryption methods to secure this data, but when we want to do the calculations on data located on a remote server, it is necessary that the cloud provider has access to the raw data, and then it will decrypt them [14].

It is an encryption algorithm that provides remarkable computation facility over encrypted data (cipher text) and return encrypted result. This algorithm can solve many issues related to security and confidentiality issues. In this algorithm encryption and decryption taking place in client site and provider site operates upon encrypted data. This can solve threat while transferring data between client and service provider, it hide plaintext from service provider, provider operates upon cipher text only. Homomorphic encryption allows complex mathematical operations to be performed on encrypted data without using the original data. For plaintexts X1 and X2 and corresponding cipher text Y1 and Y2, a Homomorphic encryption scheme permits the computation of X1 Θ X2 from Y1 and Y2 without using P1 Θ P2.The cryptosystem is multiplicative or additive Homomorphic depending upon the operation Θ which can be multiplication or addition

III COMPARISON OF EXISTING SECURITY ALGORITHM

In this section, we compare the existing symmetric algorithms on the basis of different parameters as shown in Table 1, which includes Block Size, Key Length, Security, and Speed.

Table1. Comparison of existing security algorithm of Cloud computing

S.NO	CHARACTERISTICS	DEVELOPED	BLOCKSIZE (Bits)	KEYLENGTH (Bits)	SECURITY	SPEED
	ALGORITHMS					
1.	DES	1997	64	56	Proven Inadequate	Very slow
2.	BLOWFISH	1993	64	32-448	Considered secure	Fast
3.	RC2	1987	64	8-128	High secure	Very fast

4.	RC5	1994	32, 64 or 128	MAX2040	Considered Secure	Slow
5.	RC6	1998	128	128, 192 or 256	Secure	Fast
6.	3-DES	1998	64	112, 168	Considered Secure	Slow
7.	AES	2000	128, 192 or 256	128, 192 or 256	High secure	Very fast
8.	RSA	1977	128	1024-4096	Considered secure	Very Slow
9.	DSA	1991	256	192	Secure	Fast
10.	DIFFIE-HELLMAN	1976	-	-	Not secure	Slow
11.	TWOFISH	1993	128	128, 192 or 256	Secure	Very Fast
12.	IDEA	1991	64	128	Inadequate	Slow
13.	EI GAMAL	1985	-	-	Not secure	Fast
14.	HOMOMORPHIC ENCRYPTION	1978	-	-	Secure	Fast

IV Comparative Analysis of the security algorithms

AES [15] is faster and more efficient symmetric algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. This provides high security over open network but key transfer is the major issue in symmetric algorithms.

Based on the text files used and the experimental result it was concluded [16] that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm, but RSA Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power.

Comparison of secret key and public key based DES and RSA algorithms [17], it clears that RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography. But it does not solve all the security infrastructure .So DES is used. RSA and DES differ from each other in certain features.

RSA[18] have many flaws in its design therefore not preferred for the commercial use. When the small values of p & q are selected for the designing of key then the encryption process becomes too weak and one can be able to decrypt the data by using random probability theory and side channel attacks. On the other hand if large p & q lengths are selected then it consumes more time and the performance gets degraded in comparison with DES.

According to research done [17] and literature survey it can be found that AES algorithm is most efficient in terms of speed, time, through put and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data. Based on the text files used [18] and the experimental result it was concluded that AES algorithm consumes least encryption and RSA consume longest encryption time. We also observed that Decryption of AES algorithm is better than other algorithms. From the simulation result, we evaluated that AES algorithm is much better than DES and RSA algorithm.

Homomorphic [19] cryptosystems allow for the same level of privacy as any other cryptosystem, while also allowing for operations to be performed on the data without the need to see the actual data. Complete privacy between client and server would be possible without any decreased functionality. Such systems could be applied to nearly anything that requires computation, such as voting, banking, cloud computing, and many others.

Homomorphic [20] encryption is a new concept of security which enables providing results of calculations on encrypted data without knowing the raw data on which the calculation was carried out, with respect of the data confidentiality. Security of cloud computing based on fully Homomorphic encryption is a new concept of security which is enable to provide the results of calculations on encrypted data without knowing the raw entries on which the calculation was carried out respecting the confidentiality of data.

V CONCLUSION

Data Security has become the most important issue in cloud computing security. Since, Data and Information should not be leaked to the third party user an efficient security algorithms should be implemented. This paper is a survey report on various security algorithms in cloud using cryptographic techniques. Different algorithms use different protection techniques but they all are liable to different situations. So the single security algorithms can’t be trusted. We conclude that Homomorphic algorithm is the most suitable algorithm in cloud computing environment to secure their valuable data in an open network. The ability of homomorphic algorithm to perform operations on encrypted data enables high security than other algorithms such as RSA, DES, AES. Future work is to implement hardware or software technique with Homomorphic algorithm to provide protection on cloud from any type of security attack. So we conclude that the multilevel security architecture is required for data security for each level in cloud based applications.

REFERENCES

[1] http://www.networksorcery.com/enp/data/encryption.html

[2] Dr.Chander Kant and Yogesh Sharma, “Enhanced Security Architecture for Cloud Data security” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May2013, pp. 571-575.

[3] T.Kavitha, “Cloud Computing-Brief in security algorithms”, International Journal of Research and Analytical Reviews, Volume 6, Issue 1, January 2019, pp.376-379.

[4] Balachandra Reddy Kandukuri, Rama Krishna Paturi and DR.AtanuRakshit, “Cloud security issues” In Service Computing, 2009. IEEE International Conference on, page 517520, 2009.

[5] Yogesh Kumar, Rajiv Munjal and Harsh Sharma, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures” IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[6] Mr. Gurjeevan Singh, Mr.Ashwani Singla and Mr. K S Sandha “Cryptography Algorithm Compassion for Security Enhancement In Wireless Intrusion Detection System” International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[7] Mr.MilindMathur and Mr. AyushKesarwani “Comparison between DES, 3DES, RC2, RC6, Blowfish and AES” Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[8] D.S. Abdul. Elminaam, H. M. Abdul Kader and M.M. Hadhoud “Performance Evaluation of Symmetric Encryption Algorithms”, Communications of the IBIMA Volume 8, 2009.

[9] Gurpreet Singh, Supriya Kinger “Integrating AES, DES, and 3-DES Encryption Algorithm for Enhanced Data Security” International Journal of Scientific & Engineering Research, volume 4, Issue 7, July-2013.

[10] Uma Somani, “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing”, 2010 First International Conference On parallel, Distributed and Grid Computing (PDGC-2010).

[11] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei,and Habeeb Omotunde “Diffie-Hellman and Its Application in Security Protocols” International Journal of Engineering Science and Innovative Technology Volume 1, Issue 2, November 2012.

[12] Mr. Mukta Sharma and Mr. Moradabad R. B. “Comparative Analysis of Block Key Encryption Algorithms”International Journal of Computer Applications (0975 – 8887) Volume 145 – No.7, July 2016

[13] AshimaPansotra and SimarPreet Singh “Cloud Security Algorithms” International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360.

[14] AnnapoornaShetty , ShravyaShetty K , Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014.

[15] Shraddha Soni, Himani Agrawal , Dr. (Mrs.) Monisha Sharma, "Analysis and Comparison between AES and DES Cryptographic Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

[16] Shashi Mehrotra Seth, Rajan Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, June 2011 [12]. Aman Kumar, Dr. Sudesh Jakhar, Mr. Sunil Makkar, "Comparative Analysis between DES and RSA Algorithm's", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[17] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications (0975–8887) Volume 67–No.19, April 2013

[18] Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013

[19] Liam Morris, "Analysis of Partially and Fully Homomorphic Encryption",ochester Institute of Technology, Rochester, New York

[20] Iram Ahmad and Archana Khandekar "Homomorphic Encryption Method Applied to Cloud Computing" International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.