A REVIEW ON DATA ENCRYPTION ALGORITHM IN CLOUD COMPUTING

Miss Pulatsya Kanasagara[1], Prof. Tushar J Raval[2], Prof. Karishma A chaudhary[3]

[1] *M.tech Student, Computer engineering, L.D. College of Engineering , Gujarat, India*
[2]*Associate Professor, Computer Engineering Department, L D College of Engineering, Gujarat, India*
[3] *Assistant Professor, Computer Engineering Department, L D College of Engineering, Gujarat, India*

ABSTRACT

Cloud computing provides an illusion to the customers of using infinite computing resources that are available from anywhere, any time on demand. Cloud computing provide secure data transmission. Security of data becomes a large concern to insure various attribute like integrity, confidentiality, authentication etc. .cryptography techniques like DES,Blowfish,RC5, AES, RSA, 3DES ,Diffie-Hellman plays a major roles in protecting the data in those application which are running in a network environment. In this paper providing comparative analysis on various security algorithm which are already available.

Keyword *cloud computing , cloud security , encryption algorithm*

1. INTODUCTION

Cloud computing is delivery of computing services- servers , storage , databases , networking , software etc. Various companies provides services are called cloud providers and typically charges based on usage . Cloud computing mostly used in creating new apps , to store and recover data , deliver software on demand etc.

Types of Service models provided by cloud are described below:

Software as a service (SaaS): SaaS is a software delivery model that provides access to software and its functions operating on a remote cloud infrastructure offered by cloud providers. Salesforce.com offering in the customer relationship management (CRM) space was the innovator to provide software as a service. Other examples include online word processing and spreadsheet tools, Gmail, WhatsApp, and SAP.

Platform as a service (PaaS): PaaS provides the framework for deploying and delivering of applications and services. It allows developers to develop new applications without any pressure of buying expensive tools and managing the local servers. Examples include Hadoop, Microsoft Azure, Force.com, and Google App engine.

Infrastructure as service (IaaS): IaaS provides the infrastructure such as network, memory, storage, processor to the users on demand. Examples include Amazon EC2, Windows Live Skydrive, and Rackspace Cloud.

Deployment models identified for cloud architecture are described below:

Public Cloud – The pubic cloud refers to sharing of computing infrastructure by many customers and they have no control and visibility over the computing resources where infrastructure is hosted.

Private Cloud – The private cloud does not share infrastructure with other organizations and dedicate to the particular organization. In terms of security and cost, a private cloud exceeds public clouds.

Hybrid cloud – The hybrid cloud makes usage of both of the clouds discussed above. Organizations may host less critical data on the public cloud and confidential data on the private cloud.

Community Cloud - The community cloud is used where several organizations share the similar infrastructures. It may exist on premise or off premise.

Generally, several cloud data storage concerns can arise. Typically, users will know neither the exact location of their data nor other sources of the data collectively stored with theirs.

To secure the Cloud means secure the treatments and storage " databases hosted by the Cloud provider" .Security goals of data include three points namely: Confidentiality, Integrity, and Availability (CIA). Confidentiality of data in the cloud is accomplished by encryption/ Decryption process.

This paper primarily aims to give an introduction about cloud security algorithms and comparative analysis of various encryption algorithm is also presented. This paper is arranged in as follows Section 1 Introduction .Section 2 description of existing algorithm. Section 3 comparative analysis of encryption algorithm. Section 4 conclusion.

2.EXISTING ALGORITHM ON CLOUD SECURITY

Many organisations and people store their important data on cloud and data is also accessed by many persons, so it is very important to secure the data from intruders. To provide security to cloud many algorithms are designed. Some popular algorithms are:-

2.1 *Data Encryption Standard (DES)*

This 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.

Algorithm:

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

2.2 *Advance Encryption Algorithm (AES)*

(Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. 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. It has variable key length of 128, 192, or 256 bits; default 256. It 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. Also, AES has been carefully tested for many security applications.

2.3 Triple- DES (TDES)

This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.

Algorithm:

For j = 1 to 3
{
$C_{j,0} = IV_j$
For i = 1 to n_j
{
$C_{ji} = E_{KEY3}(D_{KEY2}(E_{KEY1}(P_j, iC_{j, i-1})))$
Output $C_{j, i}$
}
}

2.4 Blowfish Algorithm

This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneier. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. 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.

Algorithm:

Divide x into two 32-bit halves: **x**L , **x**R
For i = 1to 16:
xL = **x**L XOR Pi
xR = F(**x**L) XOR **x**R
Swap **x**L and **x**R Next i
Swap **x**L and **x**R (Undo the last swap.)
xR = **x**R XOR P17
xL = **x**L XOR P18
Recombine **x**R and **x**L

2.5 RSA

This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption.

Algorithm

Key Generation: KeyGen(p, q)

Input: Two large primes – p, q
Compute n = p. q
$\varphi(n) = (p-1)(q-1)$
Choose e such that $\gcd(e, \varphi(n)) = 1$

Determine d such that e.d ≡ 1 mod φ (n)
Key:
Public key = (e, n)
Secret key= (d, n)
Encryption:
c = me mod 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 ci = E (mi) = mie mod n, then (c1. c2) mod n = (m1 . m2)e mod n

2.6. Diffie- Hellman Key Exchange

Diffie– Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie– Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communication using a symmetric key cipher.

3. COMPARATIVE ANALYSIS OF VARIOUS ENCRYPTION ALGORITHM

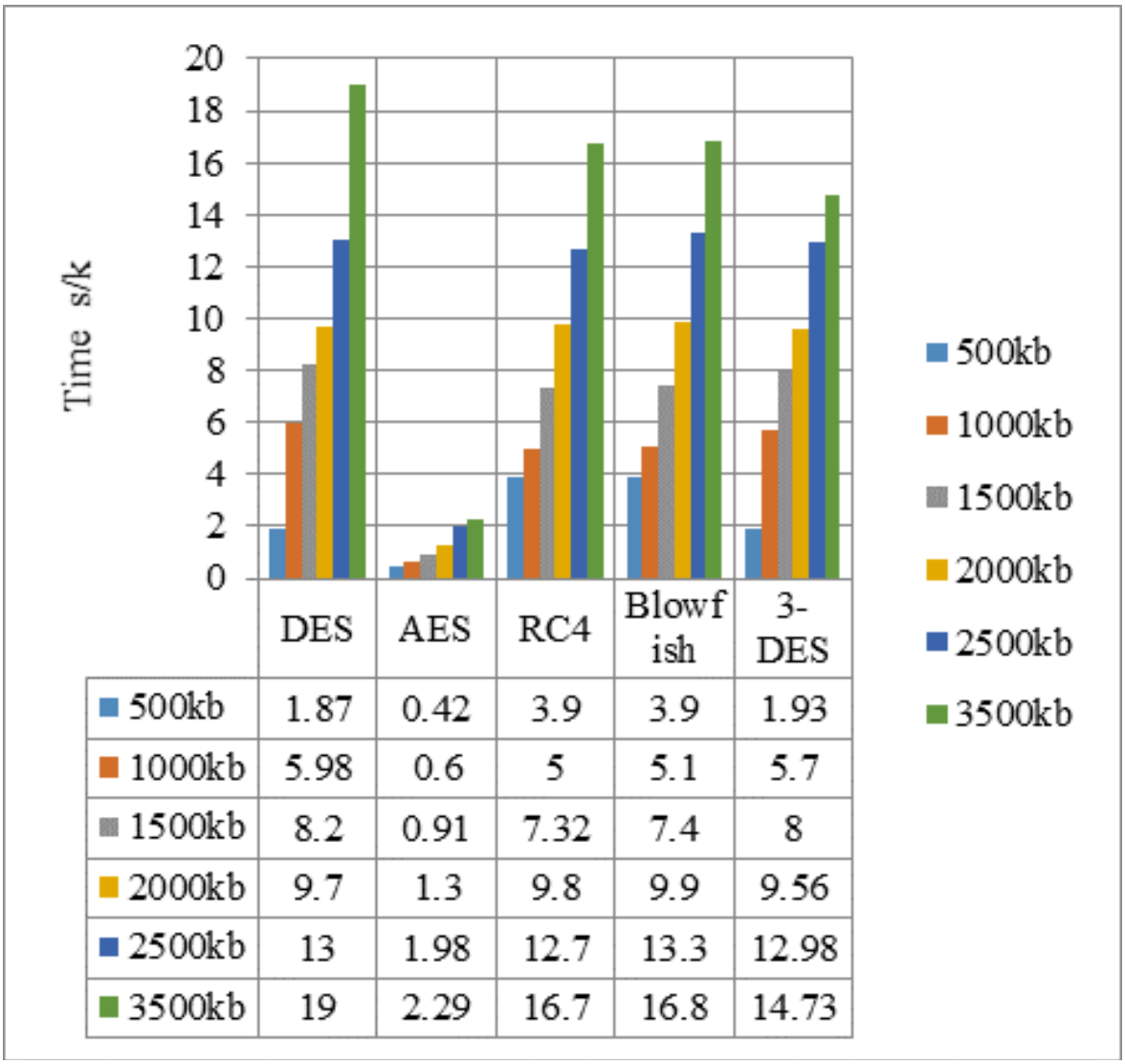
3.1 Table 1 :- Comparative analysis of algorithm

Algorithm	DES	3 DES	AES	Blowfish	RC5	RSA	DSA	Diffie-Hellman
Developed	IBM in 1975	IBM in 1978	Joan Daeman, Vincet Rijmen in 1998	Bruce Schneir in 1998	Ronald Rivest in 1994	Ron Rivest, Adi Shamir, Leonrd Adleman in 1977	NIST in 1991	Whitfield Diffie & Martin Hellman in 1976
Key Size	56	112	128, 192, 256	32-448	128	1024-4096	-	1024
Block Length	64	64	128	64	64	-	-	-
Rounds	16	48	10, 12, 14	16	12	1	-	-
Security	Proven Adequate	Considered Secure	Considered Secure	Considered Secure	Considered Secure	Considered Secure	-	-
Computational Speed	Fast	Moderate	Fast	Very Fast	Fast	Fast		
Cipher Type	Block	Block	Block	Block	Block	Asymmetric Block	-	-
Algorithm Structure	Balanced Feistel Network	Feistel Network	Substitution Permutation Network	Feistel Network	Feistel Network	-	-	-
Encryption	Medium	Low	High	Very High	High	High	-	-
Decryption Throughput	Medium	Low	High	Very High	-	-	-	-
Power Consumption	Low	High	Low	Very High	Low	High	-	-
Memory Usage	High	Very High	Medium	Very Low	Low	-	-	-
Security against attacks	Brute Force	Brute Force, Chosen Plaintext, Known Plaintext	Brute Force	Dictionary Attack	Brute Force	Brute Force, Timing Attack	-	Logjam Attack
Confidentiality	Low	High	High	Very High	High	High	-	-
Security / Comments	DES is the first encryption standard to be recommended by NIST. Many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher.	Triple DES systems are more secure than single DES. Slower than single DES.	Stronger and faster than 3DES	Blowfish is a variable length key, block cipher. Blowfish is the better than other algorithms in throughput, processing time and power consumption	Variable key size, byte-oriented stream cipher. Widely used (web SSL/TLS, wireless WEP).	RSA is slower than certain other symmetric cryptosystems. Security of RSA relies on the computational difficulty of factoring large integers	Uses exponentiation in a finite. Based on difficulty of computing discrete logarithms.	Widely used, e.g. in Secure Shell (SSH), Transport Layer Security (TLS), and Internet Protocol Security (IPSec). Limitation is lack of authentication.

Table 1 :- comparative analysis of algorithm

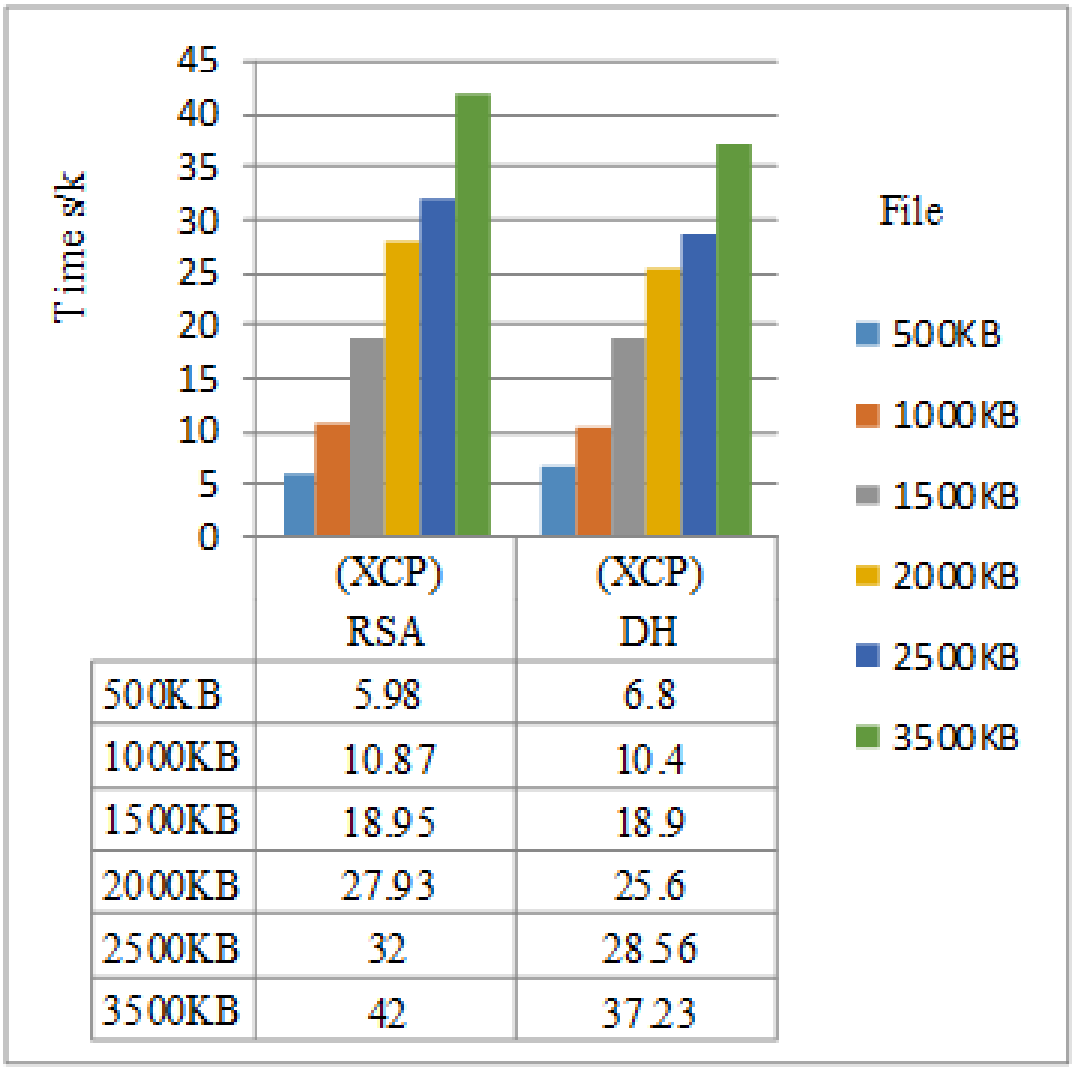
3.2 Performance analysis of algorithm

This subsection will distinguish between the two different types of encryption categories by implementing symmetric and asymmetric algorithms on the cloud network. In the following analysis both the symmetric and asymmetric techniques have been implemented using several input file sizes: 500kb, 1000kb, 1500kb, 2000kb, 2500kb, and 3500kb. Figure (3) represents the running time of the implemented symmetric techniques using the cloud network, the running time is calculated in seconds and the Input size is taken in kilobytes.



	DES	AES	RC4	Blowfish	3-DES
500kb	1.87	0.42	3.9	3.9	1.93
1000kb	5.98	0.6	5	5.1	5.7
1500kb	8.2	0.91	7.32	7.4	8
2000kb	9.7	1.3	9.8	9.9	9.56
2500kb	13	1.98	12.7	13.3	12.98
3500kb	19	2.29	16.7	16.8	14.73

Fig 1 . Running time of symmetric algorithm



	(XCP) RSA	(XCP) DH
500KB	5.98	6.8
1000KB	10.87	10.4
1500KB	18.95	18.9
2000KB	27.93	25.6
2500KB	32	28.56
3500KB	42	37.23

Fig 2 . Running time of asymmetric algorithm

4. CONCLUSIONS

Cloud computing allows consumers to use applications without installation and access their personal files at any computer with internet access. In cloud computing technology there are a set of important policy issue, which includes issue of privacy, security, anonymity, telecommunications capacity, and reliability among others. But the most important between them is security and how cloud provider assures it. In this paper analyses the importance of security to cloud. We compared seven algorithms, five algorithms for symmetric algorithm and two for asymmetric algorithm for data security in cloud. Moreover, we concluded that the algorithms implemented are more efficient on cloud environment.

5. REFERENCES

[1]. 1Omer K. Jasim, 2Safia Abbas, 3El-Sayed M. El-Horbaty and 4Abdel-Badeeh M. Salem , " **Efficiency of modern encryption algorithm in cloud computing" ,** IJETTC Nov 2016

[2]. Manpreet Kaur, Kiranbir Kaur , **A Comparative Review on Data Security Challenges in Cloud Computing** " , IRJET Jan 2016.

[3]. N. Sengupta and R. Chinnasamy. **Contriving hybrid DESCAST algorithm for cloud security**. Elsevier, pp 47-56, 2015.
[4]. S.K. Sood. **Hybrid data security model for cloud**. International Journal of Cloud Applications and Computing, pp 50-59, 2013.
[5]. Sherif, Eman, Hatem, **" Modern Encryption Techniques for Cloud Computing"** , 2nd International Conference on Communication and Information Technology, Tunisia ' 2012.