ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

A Study on various Cryptographic Techniques used in Cloud Computing

[1] Mr. Girish Kumar D, [2] Dr. Rajashree V Biradar
[1] Research Scholar, Department of CSE, BITM, Ballari, Karnataka, India
[2] Professor Department of CSE, BITM, Ballari, Karnataka, India

Abstract: **- Cloud Computing (CC) is the delivery of on-demand shared computing resources to computer or other devices. CC has changed the way we think about the way we perform our day to day operation and now a day's almost all applications are using CC to meet their requirements without actually licensing or purchasing the software and also the infrastructure. There is a lot of chance to misuse of data by the third party (Cloud Service Provider) and the main security factors which affect the performance of the system are confidentiality, availability and integrity of data. Many encryption algorithms have been developed and implemented to provide security for the data which is stored in the cloud, but no algorithm provides 100% security for the data which is stored in the cloud. This paper gives a study of different encryption techniques used in CC that is used to provide security for the data stored in the cloud.**

***Keywords*: - CC, Encryption Algorithm, etc.,**

I. INTRODUCTION

After Computers were introduced, it has become mandatory for the need of automated tools for protecting files and other information stored on the disk. Network term is misleading since all people started communicating electronically everyday by various means like e-mails, ATM's, e-commerce or mobile phones and because of that there is a rapid increase of information transmitted electronically resulted in the increase of dependence on cryptography for secure communication.

II. CLASSIFCATION OF CRYPTOGRAPHIC ENCRYPTION ALGORITHMS

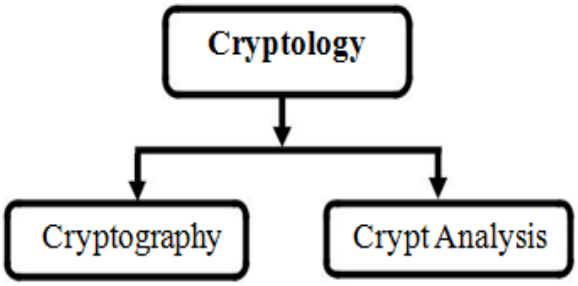

Figure 1: Classification of cryptographic encryption algorithm.

Cryptology is the study of codes or art of writing number theory, formulas and algorithms to solve them. Cryptology can be classified into two categories [1] that are cryptography and cryptanalysis.

Cryptanalysis: It is a study of cipher text which is used to identify the weakness in it and access the data without using the key or the algorithm. Cryptography: It is a science of using number theory or mathematics to hide the data by encrypting and decrypting. It is a technique used to secure data during transmission in the presence of third party. Cryptography can be further classified into symmetric ciphers and asymmetric ciphers.

Symmetric ciphers uses only one key to encrypt or decrypt a message that is private key ciphers or shared key ciphers or one key chipper or secret key ciphers.

Asymmetric ciphers use public key encryption and this algorithm requires two separate keys, one is private and the other is public. Even though both are different but still they are linked [2][3].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

Table 1: Comparison of Symmetric and Asymmetric Ciphers

Criteria	Symmetric Key	Asymmetric Key
Procedure	Same keys are used by both the users	Two different keys are used by both the users
Advantages	Safe and faster	Lets the other person read the encrypted message and there is no problem for the distributed key
Disadvantages	Both the users has to repeatedly change the key, it is one time transaction	Big and slow
Security	Moderate	Highest
Nature	Closed	Open
Key distribution	Difficult	Easy
Encryption and decryption	Faster	Slower

III. SYMMETRIC KEY ENCRYPTION

In symmetric ciphers both the uses only one key to encrypt or decrypt a message that is private key ciphers or shared key ciphers, the key may be similar or it may be simple transformation to go between the two keys.

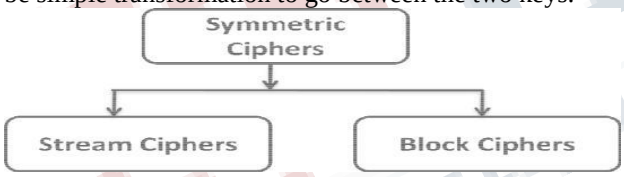

Figure 2: Symmetric key encryption algorithms.

Symmetric key encryption can be either stream ciphers or block ciphers.

Stream ciphers: It divides the text into small blocks and each block depends on many previous blocks. It encrypts bits individually and this is achieved by adding a bit from a key stream to a plain text bits. Stream ciphers can be classified into synchronous and asynchronous stream ciphers.

Block ciphers: In block ciphers a set of number of bits are grouped together into block and generally 64 bits is the size of single block. Here each block is encoded separately which depends on the previous block and same key is been used for each block. Stream ciphers are faster and have simple hardware than block ciphers.

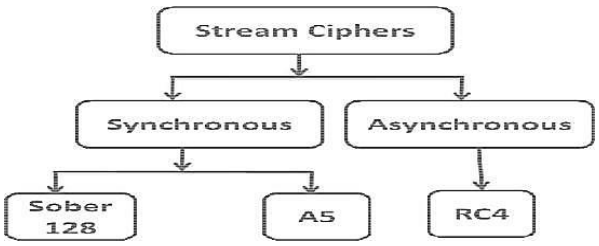

Figure 3: Stream ciphers

Synchronous stream ciphers: In this the key is generated independently of the plain text and the key stream depends only on the key. There are two properties of synchronous stream ciphers

1) The encoder and decoder must be synchronized that is the decoder must always make sure that it applies the right element of the key sequence to the given element of the ciphers text sequence.

2) If an element of the cipher text sequence has been changed (but not deleted) then only the corresponding plain text element is affected.

SOBER: It is a stream cipher designed to meet the requirements such that it should be faster than block ciphers, easy to use correctly, well understood, freely available. SOBER 128 is the latest algorithm in t5he SOBER family which is the modified version of SOBER – t32 and also used for MAC generation. This algorithm is unclear because its not be evaluated.

A5-1: It was developed in 1987 which is based on the original A5 algorithm that ensures communication confidentiality and privacy for conversations in GSM mobile phones over the air. Several ciphers were designed to handle several attacks but only few of those were implemented.

A5-2: This encryption technique is weaker when compared with A-3. The main flaw for attack is that it uses same key whether the phone encrypts using A5-1, A5-2 or A5-3 algorithm and there is lot of chance for man in middle attack by using fake base station.

A5-3: To provide signaling protection over voice calls this encryption is been used. This algorithm provides GSM users with an even higher level of protection against eavesdropping. GSM uses A5 stream generator to encrypt the digital data of the user which is transmitted between mobile station and base station and vice versa in order to avoid attacks such as a) Time memory trade-off attacks and b) Divide and conquer attacks.

A5-4: This algorithm has longer keys which provide higher level of protection to the user data which is transmitted by the GSM phone. In case of A5-3 the external input key length is 64 bits where as in A5-4 the key length is 128bits.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

This algorithm is implemented in the handset by focusing on reduction of area. Asynchronous stream ciphers: Here the key stream depends on the key stream and the cipher text.

RC4: RSA security has designed this algorithm which is simple and effective design and has variable key size which is in between 40bits and 256bits. Here the algorithm is divided into two

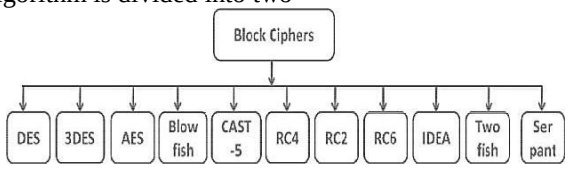

Figure 4: Block ciphers

DES (Data Encryption Standard): This algorithm was mainly used to protect passive and active attacks in communication and computer system. The security provided by this algorithm depends on key length, key management, mode of operation and implementation. It is a 64bit block cipher and the plain text is encrypted using 56 bit internal key by doing permutation and substitution and block ciphers are completely secure which is been proved.

3DES: This algorithm is still widely used because of its speed and security nature. This is the only algorithm which has 64bit (eight characters) block ciphers and there is no way that you can break DES. The memory required is further reduced since it uses two different keys. The advantage 3DES is it can be used for Authentication, Integrity, Non repudiation and Confidentiality. But the disadvantage is that it is too time consuming.

AES: The security provided by AES is related with both time and cost. It's important to know how long it will take to find the key by the attacker with high cost. Under some assumption the attacker may take 1000000000000000000000000 years to find the weakness of AES algorithm [4]. The main thing which has to be considered before using this algorithm is to decide that how long security is needed and also based on the cost. No one has proved still a way to find the weakness of this algorithm other than brute force technique.

Blowfish: This algorithm can be used as alternative for the above mentioned symmetric block ciphers which uses variable length keys ranging from 32 to 448 bits. This algorithm can be used for both domestic and exportable applications. Because it uses variable length keys this algorithm is faster than other symmetric block ciphers algorithms and it is open source. But this is very efficient if it is applied over large microprocessors. This algorithm is widely used in applications where the key will never change [5].

CAST (Carlisle Adams/Stafford Tavares): This algorithm is applied on block ciphers ie family of block ciphers. Each individual ciphers have different names such as CAST-128, CAST-256 which takes the key size such as 128, 160, 192, 224 and 256 bits respectively. CAST is been widely used by all users on royalty bases used in all applications such as commercial and non commercial. The main advantage is that it is based on the fiestel ciphers structure in which the encryption and decryption algorithms are very similar, even identical in some cases, requiring only a reversal of the key schedule.

IDEA (International Data Encryption Algorithm): The main idea behind this algorithm is the design which is innovative in nature, which uses 3 different algebraic groups and then the operations is been applied on these selected groups. This algorithm is very effective for protecting the data which is transmitted and also data which is stored which avoids unauthorized access by other users. This property of this algorithm makes difficult to crack the code.

RC2 (Rivest cipher): RC2 is very unique when we consider its design features and it is very efficient for 16 bit processors which use effective in terms of key. The main weak version of this algorithm occurs when 40 bit key is been used because the encrypted key which is been generated is been very small but still it is been used by governments as it can be easily cracked [6].

RC5: It is a parameterized algorithm which is very simple and fast enough when compared to other algorithms. The unique feature of this algorithm is it follows word oriented approach. This algorithm is adoptable even if the processor uses different word length. The beauty of this algorithm is its simplicity of its structure and it is easy to implement the task using the strength of the algorithm which provides high security when a suitable values for a parameter is been chosen.

RC6: The structure of RC6 is very simple and uses a block size of 128 bits which in turn supports different key sizes such as 128bits, 192 bits & 256 bits. This algorithm suits well for many different kinds of applications. For both encryption and decryption the key set is been made written less than 256 bytes of code. RC6 provides better performance and helps to improve the security by considering its flexibility.

Serpent: It is based on bit slicing technique which is applied over ciphers in order to get extra speed. Serpent uses single block to be encrypted by bit slicing which allows usual modes of operations such that there is no need to change the

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

environment in order to gain extra speed. The design of serpent makes very efficient use of parallelism which gives high performance [7]. The speed of dynamic serpent is twice and the size required is half to that of static design and it is open source. Twofish: It was mainly designed to be used as a replacement of AES and it has a block size of 128 bits and can accept a key length of 256 bits.

$$F : \{0,1\}^{n/2} \times \{0,1\}^{N} \mapsto \{0,1\}^{n/2}$$

Twofish also uses "prewhitening" and "postwhitening which adds an extra round of difficulty to break this algorithm. Twofish is the fastest among all AES algorithms on all CPU's [8].

Table 2: Comparison of Symmetric key cryptographic algorithms

Year	Algorithm	Possible keys	Block size	Key length	Security	Speed	Type
1974	Two fish	2^{256} bits	128 bits	128, 192, 256 bits	Considered secure	fast	Block ciphers
1977	DES	2^{56} bits	64 bits	56 bits	Proven Adequate	Very slow	Block ciphers
1978	3DES	2^{168} or 2^{112}bits	64 bits	112, 168 bits	Considered secure	slow	Block ciphers
1987	A5	2^{64} bits	64 bits	64bits	Strong	fast	Stream ciphers
1989	RC2	2^{128} or 2^{192}bits	64 bits	128 bits	Vulnerable	slow	Block ciphers
1991	IDEA	2^{128}bits	64 bits	128 bits	Considered secure	fast	Block ciphers
1993	Blowfish	2^{32} to 2^{448}bits	64 bits	32-448 bits	Vulnerable	fast	Block ciphers
1994	RC4	2^{2048}bits	64bits	256bits	Strong	fast	Stream cipers
1994	RC5	2^{2040} bits	32,64 or 128 bits	Max 2040 bits	Considered secure	slow	Block ciphers
1997	CAST 5	2^{128}bits	64bits	40-128bits	Considered secure	fast	Block ciphers
1998	RC6	2^{128}, 2^{192}, 2^{256}	128bits	128, 192or 256bits	Vulnerable	slow	Block ciphers
1998	SOBER	2^{128}, 2^{256} bits	128bits	128, 256bits	Vulnerable	fast	Stream cipers
1998	Serpant	2^{256} bits	128 bits	256bits	Considered secure	fast	Block ciphers
2000	AES	2^{128}, 2^{192}, 2^{256}	128,192 or 256 bits	128, 192 or 256	Considered secure	Very fast	Block ciphers

IV. ASYMMETRIC KEY ENCRYPTION

Asymmetric ciphers use public key encryption and this algorithm requires two separate keys, one is private and the other is public.

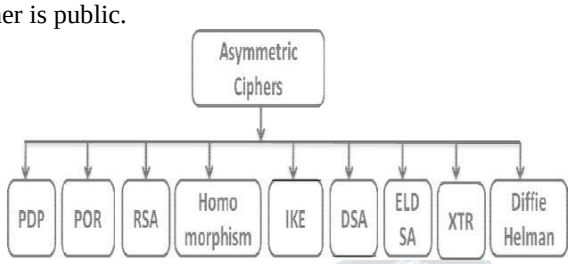

Figure 5: Classification of Asymmetric Key Encryption

Deffie Hellman: The main aim of this algorithm is to generate only one private cryptographic key for user at both the ends. This technique does not require prior knowledge with both the parties before communication. This algorithm is bit slow, but so popular in encryption key generation. When an appropriate mathematical group is used this algorithm provides more security and is not implemented on hardware.

DSA (Digital Signature Algorithm): This algorithm uses an electronic written signature of the sender or the originators which is used to send to the third party. This looks like as if the originator has signed and sent it to the recipient. This algorithm is mainly applied on the data also the programs which is stored in the disk by this the integrity of the message can be verified at any instant of time.

ECC (Elliptic Curve Crypto System): This algorithm is based on elliptic curves which is there in mathematics in which the points location is been taken as an elliptic curve in order to encrypt or decrypt the information. It provides security in most of the wireless
communication network applications such as secure electronic mail and web browsing but this technique is not the best technique when compared with the other cryptographic techniques which are available and has a drawback. The drawback is that it increases the size of the encrypted message more significantly than RSA and also it becomes more complex to implement which increases the possibility of increase in errors which affects the security of the algorithm.

ECDSA (Elliptic Curve Digital Signature Algorithm): It is basically all about mathematics and is faster than RSA and the use of short keys which reduces the CPU wastage in many wireless communication networks applications. ECDSA is based on elliptic curve discrete logarithms and if the attacker wants to attack then it requires the knowledge

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

ECC implementation in order to break the signature of the encrypted message by using reverse calculations.
IKE (Internet Key Exchange): This algorithm is used to securely exchange the encryption keys by building a VPN tunnel. It uses two modes one is main mode and the other is aggressive mode which is used to provide authentication of key exchange [9]. This algorithm is used to dynamically establish and maintain security association and it is a set of parameter necessary for providing one-way communication between two parties who are involved in communication.

Knapsack: This algorithm selects the items in the knapsack such that their sum must be exactly same as that of the knapsack capacity. Selection of items should be made in sun a way that it should not exceed the weight of the knapsack. The major advantage of this kind of encryption is its efficiency. [10]. PDP (Provable Data Procession): The main aim of this algorithm is to verify the efficiency of the stored data in the server by the client and also checks whether the server is not cheating the clients where the clients stores a large amount of data [11]. This model provides secure remote checking of data and here the client pre-capture the tags associated with each block of a file and stores in a server. This technique ensures data integrity without actually retrieving the entire file which in multi cloud, in turn improves scalability of service and data migration.
RSA: This algorithm is widely used in most of the public key encryption techniques and uses prime numbers which is greater than 1 and whose positive factor is itself and 1. Here each number are greater than 1 and factorized as a product of the powers of the randomly selected prime numbers and this technique makes this algorithm very hard to crack. In fact RSA provides secure transmission, less secure and faster algorithm.
XTR (stands for ECSTR which is abbreviation for Efficient and Compact Subgroup Tease Representation): XTR is the first method that uses arithmetic to achieve security, without requiring explicit construction of groups. This algorithm can be used as a combination with any cryptographic technique which performs operation on subgroups and also avoids computational overhead. The security level of XTR public key system is very efficient and also reduces the amount of data storage. This algorithm is more effective where the resources are limited. Homomorphic Encryption (HE): In this algorithm the performed operation on encrypted data without actually decrypting the cipher text. HE is distinguished according to the type of operation which they perform on the plain text or raw data. HE can be further classified based on two properties ie Additive and Multiplicative. The cryptosystem which exhibits any one of the property is known as partial HE and the cryptosystem which uses both the properties is referred as Fully HE [12][13].

Table 3: Comparison of Asymmetric key cryptographic algorithms

Year	Algorithm	Advantages	Disadvantages
1937	PDP	Provides public verification with protection against small corruptions	Searching is slow & insecure for dynamic data
1976	Diffie-Hellman	The secret key is not transmitted by itself over the channel and safe against passive eavesdropping	Authentication, unsafe against active attacks
1978	Knapsack	It is a perfect protocol for secret key distribution	Sequences of deciphering keys are breakable
1985	ECC	Fast, uses short keys and less computational power	More expensive and reduces the lifetime of batteries used
1992	ECDSA	Provides secured means of communication	Key exchanging is difficult
1993	DSA	Provides authentication and integrity	The security of the private key depends upon the computer
1994	Homomorphic	Easy to maintain and provides enhanced privacy for private informational	Performance is not feasible and increase complexity

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 11, November 2017

		retrieval	
1998	IKE	Provides security without pre configuration	To establish a connection both parties should agree with the type of security association
2006	XTR	The key generation is fast and uses less keys	The user has to use different random numbers to transmit the message
2008	RSA	Authorized user can send the message	Many other secret key encryption techniques are much faster

V. COMPARATIVE ANALYSIS

Here many encryption algorithms are used and based on the techniques an analysis is been made [14][15][16]. INPUT DATA SIZE- The above mentioned all the algorithms which may take different memory space in order to perform its operation. The size of memory required by each algorithm depends upon the input data and also on the number of rounds required by each algorithm. Any algorithm which uses less memory usage uses small key length and which performs very efficiently is considered as best. TIME- The time elapsed by any algorithm to complete the task depends on processor speed, algorithm complexity. The less time an algorithm takes, the more efficient it will be when compared to others. THROUGHPUT- The throughput of any encryption algorithm is computed by splitting the entire plain text into megabytes of data, total time taken and also the size of the cipher text generated for each algorithm.

VI. CONCLUSION

This paper tries to present a study on various cryptographic techniques carried out till today in CC. The above analysis gives a quick overview of all the cryptographic techniques and a brief description on each algorithm, which helps the users to understand the difference between each algorithm

REFERENCES

[1] Suriya kala.L, Dr. R. Thangaraj "A Study on different Image Encryption Algorithms" ,(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1204-1206

[2] Swadeep Singh, Anupriya Garg, Anshul Sachdeva, "Comparision of Cryptograpic Algorithms ECC and RSA", International Journal of Computer Science and Communication Engineering (IJCSC), Special issue on "Recent Advances in Engineering & Technology" NCRAET-2013, ISSN 2319-7080.

[3] Sahan Ahmad, Kazi Md. Rokibul Alam, Habibur Rahman, and Shinsuke Tamura, "A Comparison between Symmetric and Asymmetric Key Encryption Algorithm based Decryption Mixnets", National Conference on Networkinh Systems and Security (NSysS), 2015, 978-1-4799-8162-7/2015 IEEE

[4] P. Princy, "A Comparison of Symmetric Key Algorithms Des, Aes, Blowfish, Rc4, Rc6: A Survey", International Journal of Computer Science & Engineering Technology (IJCSET) ISSN: 2229-3345 Vol. 6 No. 05 May 2015

[5] Tingyuan Nie and Teng Zhang, "A Study of DES and Blowfish Encryption Algorithm", IEEE Region 10 Conference (TECHNO) IEEE, 2009.

[6] R.L. Rivest."The RC5 encryption algorithm". In B. Preneel, editor, Fast Software Encryption, volume 1008 of Lecture Notes in Computer Science, pages 86-96, 1995. Springer Verlag.

[7] Neeta Wadhwa, Syed Zeeshan Hussain & S. A. M Rizvi, International Journal of Computer Science and Engineering (IJCSE) ISSN 2278-9960 Vol. 2, Issue 3, July 2013, 89-94

[8] V. Mnssvkr Gupta, K.V.S. Murthy, A. Yesubabu, R. Shiva A Shankar, "Recent performance evaluation among various AES algorithm- MARS, RC6, RIJNDAEL, SERPENT, TWOFISH", International Journal of Science and Advanced Technology(IJSAT), 2012.

[9] Perlman, R. and Kaufman, C. "Key Exchange in IPSec: Analysis of IKE", IEEE Internet Computing, Nov/Dec 2000.

[10] M. S. Hwang, C. C. Lee, and S. F. Tzeng, "A New Knapsack Public- Key Cryptosystem Based on Permutation Combination Algorithm", International Journal of Applied Mathematics and Computer Sciences (IJAMCS) vol. 5; 1, pp. 33-38, Winter 2009.

[11] Pooja Natu, Prof. Shikha Pachouly "A Comparative Analysis of Provable Data Possession Schemes in Cloud", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (6), 2014, 7927-7931

[12] Xun Yi, Russell Paulet, Elisa Bertino 2014"Homomorphic Encryption and Applications", SpringerBriefs in Computer Science, DOI 10.1007/978-3-319-12229-8__2

[13] Payal V. Parmar, Shraddha B. Padhar, Shafika N. Patel, Niyatee I. Bhatt, Rutvij H. Jhaveri, "Survey of Various Homomorphic Encryption algorithms and Schemes", International Journal of Computer Applications (0975 – 8887) Volume 91 – No.8, April 2014

[14] Prashanth Kumar Arya, Dr Mahendra Sing Aswal, Dr Vinod Kumar, "Comparative Study of Asymmetric Key Cryptographic Algorithms" International Journal of Computer Science & Communication Networks,Vol 5(1),17-21

[15] S. Nithya , Dr. E. George Dharma Prakash Raj, " Survey on Asymmetric Key Cryptography Algorithms", Journal of Advanced Computing and Communication Technologies(JACCT) (ISSN: 2347 - 2804) Volume No. 2 Issue No. 1, February 2014

[16] Yogesh Kumar, Rajiv Munjal, 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 2011ISSN (Online): 2231-5268