International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

Comparative Study on Data Encryption Algorithms in Cloud Platform

D, Palanivel Rajan,
Assistant Professor – II,
Dept. of Computer Science & Engineering,
Coimbatore Institute of Engineering and Technology
Narasipuram, Tamil Nadu 641109

Dr. S. John Alexis, Professor,
Dept. of Automobile Engg,
Kumaraguru College of Technology
Chinnavedampatti, Saravanamptty,
Coimbatore-641049, Tamil Nadu 641109

***Abstract* - The high growth in the cloud computing has reached the each and every corners of the world. The cloud computing offers the dynamically shared resources namely networks, storage, servers, services and applications, without physically acquiring them. So it saves managing cost and time for organizations. Cloud services providers various services like SaaS, Paas, IaaS, NaaS and etc., over the internet. Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. Security is to save data from danger and vulnerability. There are so many dangers and vulnerabilities to be handled. There are still some challenges to be solved among that the security and trust issues are vital one. In this paper the various kinds of the encryption algorithms are discussed in details and the performances of those algorithms are evaluated to analysis the best algorithm for the cloud platform. This discusses the various open research issues and challenges that present in the cloud platform.**

Keywords: Security Issues, Cloud Security, Cloud Architecture, Data Protection, Cloud Platform, Grid Computing

I. INTRODUCTION

Cloud Computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Cloud service providers (CSP's) offer cloud platforms for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet. CSPs and ISPs (Internet Service Providers) both offer services. Cloud computing is a model that enables convenient, on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, applications that can be rapidly provisioned and released with minimal management effort or service provider's interaction. There are various reasons for organizations to move towards IT solutions that include cloud computing as they are just required to pay for the resources on consumption basis. In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers [1].

This paper is organized as below. The Section II discuss the various technical processes involved in the cryptography and the Section III discuss the various data encryption algorithms , Section IV analysis the different parameters like time taken for the encryption, e and the key size and the Section V will conclude the survey with the pointed obtained from the analysis.

II. BACKGROUND THINGS

A. *Cryptography*

Cryptography is an art of hiding information by encrypting the message. The art of protecting information it into an unreadable format possess a secret key can de-cipher the message into plain text [4].

a. *Encryption:* The Process of converting the plain text into unreadable raw text is called encryption.
b. *Decryption:* The Process of converting the unreadable text into readable plain text is called encryption.
c. *Plain text:* The original text or message used in communication in called as Plain text.
d. *Cipher text:* The plain text is encrypted in un-readable message. This meaningless message is called Cipher Text.
e. *Key:* A key is a numeric or Alpha-numeric text (mathematical formula). In encryption process it takes place on Plain text and in decryption process it takes place on cipher text.
f. *Key size:* Key size is the measure of length of key in bits, used in any algorithm.
g. *Block size:* Key cipher works on fixed length string of bits. This fix length of string in bits is called Block size. This block size depends upon algorithm.

B. *Key Goals of the Cryptography*

The major key goals of the cryptography [7] are given below.

a. *Confidentiality:* Ensuring that information is accessible only to those authorized to have access.
b. *Integrity:* It should be possible for the receiver of a message to verify that it has not been modified in transit. An intruder should not be able to substitute a false message for a legitimate one.
c. *Non-repudiation:* A sender should not be able to falsely deny later that he sent a message.
d. *Authentication:* It should be possible for the receiver of a message to ascertain its origin. An intruder should not be able to masquerade as someone else.
e. *Access Control:* The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

III. RELATED WORKS

A. Types of encryption algorithm

Data Encryption (Cryptographic) Algorithms are classified into two types as follow.

A. Symmetric

In this kind of cryptography for both encryption and decryption a single key is used. And same key should be known to both sender who encrypts the message and the receiver who decrypts. DES, Triple DES, AES, RC5, etc al be the example of such encryption [9].

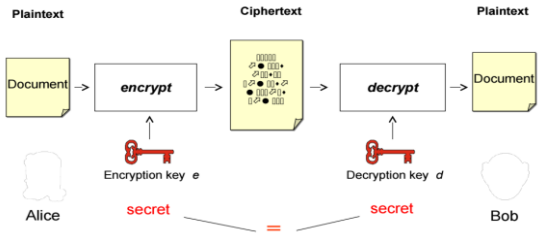

Figure 1. Symmetric Encryption Algorithm

i DES: The Data Encryption Standard (DES) was once a predominant symmetric-key algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world [11].

ii Triple DES: The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm [14].

iii RC4: RC4 (Rivest Cipher 4) is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems [8]. It is especially vulnerable when the beginning of the output key stream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP.

i. SHA-I: SHA stands for "Secure Hash Algorithm", SHA-1 is cryptographic hash function technique where hash of data is computed [6]. AS compared to SHA-0, SHA-1 is widely used because it corrects errors in SHA hash specification, which led to weakness.

ii AES: The Advanced Encryptions Standard (AES) is a symmetric key encryption/decryption algorithm for converting plain-text to cipher text and vice-versa [2]. Since the same key or master key is used, the must be kept secret or with trusted 3rd party, because compromise of this key would mean compromise to the data.

B Asymmetric

Different key is used for both encryption and decryption in this cryptographic algorithm. Message sender encrypts the message or data using public key that may be known to all publicly [10]. On the other side message receiver uses other secret key to decrypt the message.

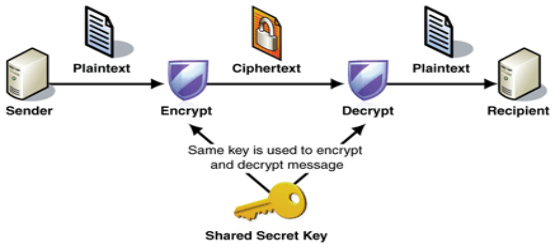

Figure 2. Asymmetric Encryption Algorithm

In this cryptography both public and private key can be used only for one purpose. RSA, Elliptic Curve, etc may be the examples of such Encryption. Different key is used for both encryption and decryption in this cryptographic algorithm. Message sender encrypts the message or data using public key that may be known to all publicly. On the other side message receiver uses other secret key to decrypt the message. In this cryptography both public and private key can be used only for one purpose. RSA, Elliptic Curve, etc may be the examples of such Encryption[12].

B. RSA: This is a web secret authentication system that uses an algorithmic program developed in 1977 by Ron Rivest, Adi Shamir, and author Adleman. The RSA algorithmic program is that the most typically used in secret writing. until currently it's the sole algorithmic program used for personal and public key generation and secret writing. it's a quick encryption [13].

C. DSA: The Digital Signature algorithm (DSA) may be a Federal science normal for digital signatures. it absolutely was projected by the National Institute of normal and Technology (NIST) in August 1991 to be used in their Digital Signature Standard (DSS) With DSA, the entropy, secrecy, and individualism of the random signature price k is crucial [3]. it's therefore crucial that violating anyone of these 3 necessities will reveal the complete personal key to an assaulter. Exploitation a similar price doubly (even whereas keeping k secret), employing a inevitable value, or leaky even many bits of k in every of many signatures, is enough to interrupt DSA.

Diffie-Hellman: Diffie–Hellman key exchange [5] may be a specific methodology of exchanging cryptologic keys. it's one among the earliest sensible samples of key exchange enforced inside the sector of cryptography. The Diffie–Hellman key exchange methodology permits 2 parties that haven't any previous data of every different to collectively establish a shared secret key over an insecure communications channel. This key will then be accustomed inscribe consequent communications employing isobilateral key cipher.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

III. DISCUSSION

The both symmetric and asymmetric encryptions algorithms are compared in terms of different parameters such as key size, block size, number of rounds and the avalanche effect over the particular algorithm in the table I. Avalanche effect is a term from cryptography that describes behavior of a special kind of math functions. Even a slight change in an input string should cause the hash value to change drastically. A Hash Function is a transformation that takes a variable length bit sequence (Message) and produces a fixed length bit sequence (Message Digest). Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect, since it is computationally infeasible to produce a document that would hash to a given value or find two documents that hash to the same value, a document's hash can serve as a cryptographic equivalent of the document [15].

Table I. Comparison of Encryption Algorithm

Encryption Algorithms	Key size (bits)	Block size (bits)	No of rounds	Avalanche Effect
DES	56	64	16	Less than AES
Triple DES	112 or 168	64	48	Medium
RC4	40-2048	NA	1	Fast encryption /decryption compare to DES
SHA-I	384	512	80	Fast when compare to triple DES.
AES	256	128	10,12,14	Fast encryption/decryption. Less than des
RSA	>1024	Min 512	No Rounds	Fast encryption and decryption when key size is low
DSA	512 to 1024	NA	1	Faster than RSA
Diffie-Hellman	3072-bit or larger	NA	1	Less than SHA-I

This makes a one-way hash function a central notion in public-key cryptography. When producing a digital signature for a document, we no longer need to encrypt the entire document with a sender's private key (which can be extremely slow). It is sufficient to encrypt the document's hash value instead. The time taken to encrypt the raw file is calculated in the cloudsim platform for the various file size like 32, 64,128,256,512(in MB) is calculated and presented in the table II. The same represented in the figure 3. The standard deviation of the encryption time for the various algorithms is represented in the figure 4.

Table II. Encryption Algorithm with key size in bits

File Size (In Mb)	Encryption Time (in Milliseconds)							
	DES	Triple DES	RC4	SHA-I	AES	RSA	DSA	Diffie-Hellman
32	272	788	198	1264	238	274	392	483
64	1253	1095	372	4125	595	359	530	895
128	2586	3810	763	6024	960	461	1104	1248
256	6034	7628	1253	8474	1688	519	1837	2872
512	8436	11038	2595	10567	2122	984	2302	3408

The DES have the mean of 3716, median of 2586 and the standard deviation of 3423. its uses the 56 bits key with 16 makes its secure at the same time encrypt the data fast when compare to the triple DES. Triple DES has the mean of 4872, median of 3810, and the standard deviation 4407. Its uses the 112 or 168 bit key with 48 rounds makes its strong enough against the attacks at the same time this takes long time to encrypt the file when compare to all other algorithms.

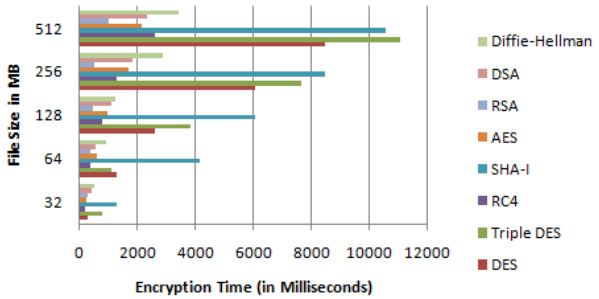

Figure 3. Encryption Time for the various Algorithms

RC4 have the mean 1036, median of 763 and the standard deviation of 961. Its uses the key ranges from the 40 to 2048 bits and runs only single round, which makes this as faster one when compare to the DES and triple DES.

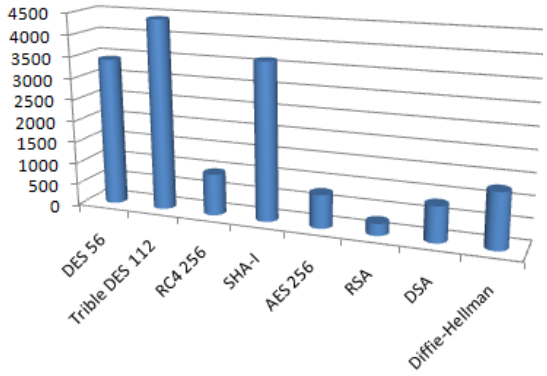

Figure 4. Standard Deviation of the various Algorithms

SHA-I have the mean 6091, median of 6024 and the standard deviation of 3636. Its use the key of 384 bits with 80 rounds make it harder , takes less time when compare to triple DES. AES have the mean 1121, median of 960 and the standard deviation of 776. Its uses the 256 bit key with 10 or12 or 14 rounds provides the fast encryption when compare to the DES, triple DES and SHA-I. ***RSA*** have the mean 519, median of 461 and the standard deviation of 276. Its uses the key size more than the bits and the process the input as blocks of minimum size 512 makes it fast. but the encryption time propositionally increase based on the key size..

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 10, October - 2017

DSA have the mean 1233, median of 1104 and the standard deviation of 825. its uses the keysize range from the 512 to 1024 bits with the single round makes it more secure and less time consumption when compare to the AES and RSA. *Diffie-Hellman* have the mean 1781, median of 1248, and the standard deviation of 1284. Its uses the large keysize the i.e., the minimum key size is 3072 bits and the single round makes its more secure than the RSA and DSA but this process takes the large time when compare to AES , RSA and DSA.

IV. CONCLUSION

This paper presents a detailed study of the popular Encryption Algorithms such as RSA, DES, 3DES and AES in the cloud platform. There are more requirements to secure the data transmitted over different networks using different services. To provide the security to the network and data different encryption methods are used. In this paper, a survey on the existing works on the Encryption techniques has been done. To sum up, all the techniques are useful for real-time Encryption. Each technique is unique in its own way, which might be suitable for different applications and has its own pro's and con's. According to research done and literature survey it can be found that AES, RC4 and Diff-Hellman algorithms are most efficient in terms of time and avalanche effect. The Security provided by these algorithms can be enhanced further, if more than one algorithm is applied to data.

Our future work will explore this concept and hybrid approach using nature inspired algorithm to find the suitable encryption algorithm on the fly, based the current environment needs to ensure the security and increase the performance.

REFERENCE

[1]. A. Hasib and A. A. M. M. Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography," Convergence and Hybrid Information Technology, 2008. ICCIT '08. Third International Conference on, Busan, 2008, pp. 505-510.

[2]. M. Yeşiltepe, E. Kaçmaz and M. Kurulay, "Study triple data encryption standart encryption algorithm in windows communication foundation environment," 2016 Electric Electronics, Computer Science, Biomedical Engineerings' Meeting (EBBT), Istanbul, 2016, pp. 1-4.

[3]. K. Zeng, C. H. Yang, D. Y. Wei and T. R. N. Rao, "Pseudorandom bit generators in stream-cipher cryptography," in IEEE Computer, vol. 24, no. 2, pp. 8-17, Feb. 1991.

[4]. E. F. Brickell and A. M. Odlyzko, "Cryptanalysis: a survey of recent results," in Proceedings of the IEEE, vol. 76, no. 5, pp. 578-593, May 1988.

[5]. R. Mathur, S. Agarwal and V. Sharma, "Solving security issues in mobile computing using cryptography techniques — A Survey," Computing, Communication & Automation (ICCCA), 2015 International Conference on, Noida, 2015, pp. 492-497.

[6]. O.A. Hamdan and B.B. Zaidan "New Comparative Study Between DES 3DES and AES within Nine Factors" ,Journal Of Computing, vol. 2 no. 3 March 2010.

[7]. S.P. Singh and R. Maini "Comparison Of Data Encryption Algorithms" ,International Journal of Computer Science and Communication,vol. 2 no. 1 pp. 125-127 January–June 2011.

[8]. Y. Kumar R. Munjal and H. Sharma "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", International Journal of Computer Science and Management Studies, vol. 11 no. 3 Oct 2011.

[9]. P. Mahajan and A. Sachdeva "A Study of Encryption Algorithms AES DES and RSA for Security" ,Global Journal of Computer Science and Technology Network Web & Security,vol. 13 no. 15 2013.

[10]. S. Chandra, S. Bhattacharyya, S. Paira and S. S. Alam, "A study and analysis on symmetric cryptography," Science Engineering and Management Research (ICSEMR), 2014 International Conference on, Chennai, 2014, pp. 1-8.

[11]. P. Liu H. Chang and C. Lee "A true random-based differential power analysis countermeasure circuit for an AES engine" ,IEEE TRANSACTIONS on CIRCUITS and SYSTEMS-II: EXPRESS BRIEFS,vol. 59 no. 2 pp. 103-107 2012.

[12]. H. Hayouni, M. Hamdi and T. H. Kim, "A Survey on Encryption Schemes in Wireless Sensor Networks," Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on, Haikou, 2014, pp. 39-43.

[13]. G. Padmavathi and D. Shanmugapriya "A Survey of Attacks Security Mechanisms and Challenges in Wireless Sensor Networks",(IJCSIS'09) International Journal of Computer Science and Information Security,vol. 4 no. 1&2 2009.

[14]. Q. CHEN Z. TANG Y. LI Y. NIU and J. MO "Research on Encryption Algorithm of Data Security for Wireless Sensor Network" ,Journal of Computational Information Systems, pp. 369-376 2011.

[15]. M. Cakroglu C. Bayilmis A.T. Ozcerit and O. Cetin "Performance evaluation of scalable encryption algorithm for wireless sensor networks" ,Scientific Research and Essays,vol. 5 no. 9 pp. 856-861 May 2010.