IEEE Sponsored World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR'16)

Enhanced Cloud Security Framework To Confirm Data Security on Asymmetric And Symmetric Key Encryption

N.Jayapandian
Assistant Professor
Knowledge Institute of Technology
njayapandian@gmail.com

Dr.A.M.J.Md.Zubair Rahman
The Principal
Al-Ameen Engineering College,Erode
mdzubairrahman@gmail.com

S.Radhikadevi, M.Koushikaa
Knowledge Institute of Technology,Salem
njpcse@kiot.ac.in

ABSTRACT

Cloud is a modern business sharing data or information with great effectiveness of infrastructures it plays a major role in world wide. As in the information technology sector defines cloud security is the evolving sub domain of computer security and information security. Here the organization uses the cloud as a many service model (Saas ,Pass and Iass)and deployment model (private, public, hybrid and community). In this type of model the responsibilities more for secure the information of the customer, So the organization ensures the different way to monitor and secure the data and information from hacking. They offer suspicious activity for their customer data by enhancing the data with encryption and decryption. Encryption makes the access method of proving the original data to be duplicated form and then the client can also be constructed with the proper decryption of the data to prevent the information from eavesdroppers from accessing Symmetric keys encryption or secret key encryption. The Key should be distributed before transmission between entities,then key play vital role for security .DES is In Asymmetric key encryption or public key encryption on that private and public keys are used in the encryption level on cloud. The Public key is used for encrypting the file and private key is used to decrypt the file . Because user tends to use two keys public this is known to public and private who is known to the user a type of algorithm such as RSA. Here we analysis the document is encrypted and then which efficient in that way of approach.

***Index Terms* - cloud computing; HSBE; Data Encryption and; data privacy ; DES.**

I. INTRODUCTION

Technology are run in the field of internet of it service that too in Cloud Computing is the fundamental change happening in the business environment. It take part of a movement towards the intensive, IT specialization[1].Moreover, it brings about not only convenience and efficiency issues, but also great effect in the field to secure data and protection of data from hackers However, security has been regarded as one of the greatest issue in Cloud Computing. This paper describes the great needs in Cloud Computing, security key technology, standard and growth of information sensitivity .[2] This paper explains that the changes in the above aspects of security on network will result in a technical strategy in the field of data security, by using the method of data encryption and decryption[8].This scheme is traditionally prefer in the security area of data in cloud. Cloud encryption is commonly used to protect the information from the hackers and unknown member of access and also protect sensitive data stored in cloud, and enhance security for outgoing that leaves a secured network. Then we exposé to the idea of encryption. Encryption is one of the algorithm that protect the secure and more sensitive information on it. Encryption method analysis various schemes for secure the sensitive information the document(original message before encryption) and transforms it into cipher text (clamber message after encryption). There are many algorithms we implement for information. Many encryption technique are widely available on the method of data security[7].Encryption algorithms are classified into two types: Symmetric-key (secret-key) and Asymmetric-key (public-key) encryption. Symmetric key algorithm play a main role ,In practice a shared secret data between two are more storage area that can be use to maintain their own instruction of the system, that can be a number , a word or just a characters that can be applied in the text here we are highly move to the DES encryption on cloud. Asymmetric encryption algorithm or public-key encryption in which encrypt and decrypt a message so that it arrives securely and transaction on a pair of keys is used to save the statement in cloud . In this we are using both public and private key for security so it can be secure then no issue of giving public key it can be known by all then for strong security we can use private key. RSA algorithm best needed to use in public key cryptography is but it have more main in the problem of other security .It can be processes are performed through a series of modular multiplication. Are the major methods used in encryption and decryption according to the customer security.

II. PROBLEM STATEMENT

This There are various issues and defects in cloud computing sector which include privacy, segregation, storage, reliability, security. Hence in cloud most significant among these of that to be more concern in security and service provider of cloud to be allowed to manage level of the data on cloud which provide sensitive data place in the document and allowed to work by authorized[9]. Because cloud is a

978-1-4673-9214-3/16/$31.00 © 2016 IEEE

wide area where it can be act several role according to the user and provide different service to the customer. If cloud clients are in need of security effect on performance of computing and maintain their data form the cloud providers have to find different methods to combine the data to be more preserve and maintain the own content of the data and then to increase the level of performance of the document to analysis their information and encryption on the cloud has to be done For enterprises and the client of cloud, most important problem is also security because many of them are interest to hack others data for various motive so in the point of cloud is wide network area to use and communicate. So, we mainly concentrate on information security using in encryption and decryption algorithm of cloud computing sector[1]. Here many number of algorithm are used but still it not secure properly, it not concentrate on whole partially data can be secure in one level to another.[5]

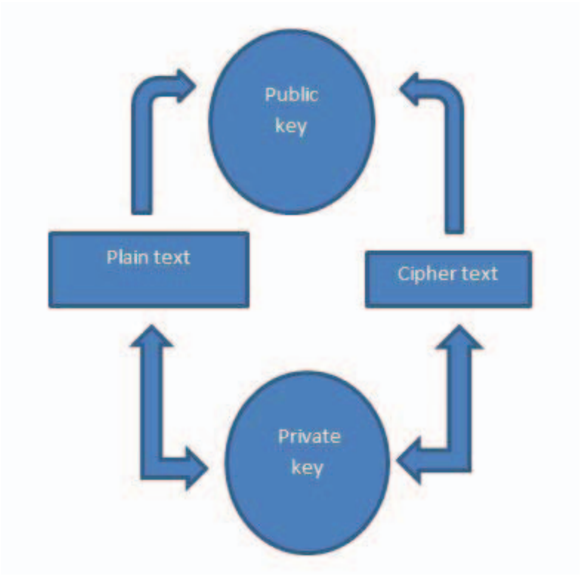

Figure 1.1: Encryption and Decryption

III. DATA ENCRPTION STANDARD ALGORITHM

The DES means of the data encryption standard on cloud. This type of algorithm in which same key is used for encryption and decryption and mainly secure by the secret key method. DES is one of the most widely accepted, publicly available encrypted systems. It was developed in 1970s by IBM corporation, but was later control by the National Institute of Standards and Technology (NIST) here that DES algorithm works by using the same key to make privacy of the instruction by the process of encrypt and decrypt a message in a system, so both the user of the domain and the provider must know and they same will use secret key for further privacy. Here, we will implement to move the document on , symmetric-key algorithm for the encryption of electronic data, DES has been done by the more secure Advanced Encryption Standard algorithm of the symmetric key process in the encryption and decryption methodology.

The Data Encryption Standard is a block cipher, meaning a encrypted key and algorithm are applied to a segment of data simultaneously process has done on one bit at a time. To encrypt a original data, DES groups it into 64-bit blocks. Each block is encrypted[3] the plain text by using the secret key into a 64-bit plaintext by means of segregation and substitution of the original information. The DES algorithm will encrypt information in the original of space used by the system is same. Here we are using the method of encryption as that 64 bit separated as the 32 bit then it named as the Right R 32 bit and Left L 32 bit plain text is M =123456 where 0001 0010 0011 0100 0111 0101 here the text can be encrypted by various technique R=0101 0111 0100 L=0001 0010 0011 so it can be splited and encrypt in various way For example replace the position of 0's and 1's from left to right.

This adversary (call it A1) will attempt to cryptanalyze its input by brute force. It has its own DES implementation. It gives a single method of the system launch in the oracle core system proved to, asked for the 64-bit string of all zeroes to be encrypted. Call the resulting ciphertext E0. It then runs an enormous speed of key search. The DES algorithm looks like this:

```
E0 = oracle_query(0)
 for k in 0,1,...,256-1:
   if DESk(0) == E0:
     return 1
     return 0
```

A. DES ALGORITHM

step1 -Take the text format as the plain text with name as
M=123
Step2-M plain split into Left and Right M-L &R
Step3-L=key can be encrypted by position. First and last
step 4=here it can be encrypted by changing 0's and 1's

DES Leader method

Leader L is derived from the Password. Here we have 16 rotations. So we need 16 Leaders (L1 to L16) from Password.

L1 = First two bits of Password
L2 = Second two bits of Password
L3 = Third two bits of Password and so on
STEPS:
Get the Plaintext.
Get the Password.
Convert the Characters into binary form.
Derive the Leaders (L1 to L16) from the Password.
Apply the Formula to get the encrypted and decrypted message.

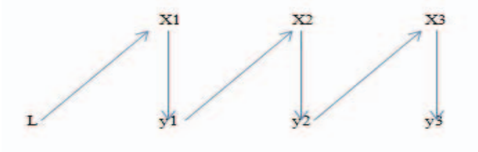

Figure 3.1 Encryption on DSE

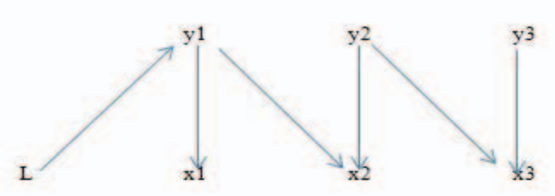

Figure 3.2 Decryption on DSE

B. RSA ALGORITHM

RSA is proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 from the asymmetric method. It is one of the best known public key for exchange or digital signatures or encryption of the process data. RSA is mainly exposing an asymmetric method in the encryption and decryption algorithm[4]. It is a method of asymmetric. technique, that here public key distributed to all through which one can encrypt data of the original message and private key which is used for decryption is maintained for more privacy to kept secret and it will not shared to every person. Here variable size encryption system and a variable size key also has been implemented in the method. The Sender encrypts the conent of the message by using the public key from the receiver and when the message gets move to receiver, next process start by the receiver can decrypt it using his own private key. RSA operations can be classified in three vital steps; key generation, encryption and decryption. RSA algorithms to find the best one security and productivity method, which has to be used in cloud for making online storage instruction to be more sensitive to secure and not to be hacked by unauthorized. Here it can be flexible to use by the user and the provider. RSA is a Block Cipher in which every message is model into an integer of the text. RSA intakes longest memory size and exceeds the encryption time. Once the data is encrypted with the Public key, it will be decrypted using the respective Private Key of the data[6]. This encryption asymmetric algorithm also plays a wide role but it can be not more secure as like symmetric encryption.so prevent we need to improve the privacy for data symmetric technology of encryption is used for sensitive data.

IV. MATHEMATICAL MODEL

A. RSA Key Generation

1)Select two random numbers p & q.

2)Compute the value of n where n=r*s

3) Compute Ø (phi) = (r – 1) (s – 1)

4) Select integer (e) so that gcd (e, Ø) = 1.

5)Compute both the value of d where (d * e) = 1 mod Ø.

B. EXAMPLE FOR SOLVING RSA IN ENCRYPTION

Choose r = 3 and s = 11 in the model we first assign he value of r ,s andCompute n = r * s= 3 * 11 = 33 on thevalue to be on the Compute φ(n) = (r - 1) * (s - 1) = 2 * 10 = 20 next aim toChoose e such that 1 < e < φ(n) and e and n are coprime. Let e = 7 thenCompute a value for d such that (d * e) % φ(n) = 1. One solution is d = 3 [(3 * 7) % 20 = 1] here we give the public key and private key then the valuePublic key is (e, n) => (7, 33) and the value of Private key is (d, n) => (3, 33) and The encryption of m = 2 is c = 27 % 33 = 29 then thevalue methodology ofThe decryption of c = 29 is m = 293 % 33 = 2.

V. COMPARITIVE STUDY OF SECURITY ALGORITHMS

Here we are secure the cloud network data by encryption by the method of symmetric and asymmetric in that proposal, We explain about an RSA algorithm which less secure than the symmetric DES algorithm. DSA and RSA are two common encryption algorithms that can be said to be of more secure and show the equal performance of the two is what differs one from the other by their performance and other strategy. RSA is not much faster when generating a key than DSA.moreover,RSA is faster at encryption than DSA method When decrypting, DSA shows their strength, mainly due to its great decryption capability If you need digital analysis method of signing, DSA is the encryption algorithm of the method in the encryption for the analysis is the process of the digital signature RSA is the best method of the verification of data. Depending on the place of usage their view of the method, will need to be done the process, but both DSA and RSA have the same level of encryption capabilities and the option with less choice of demand for the resources should be chosen. Because the way of using the level of key for security differs as they can use the key as where the place it depend on usage of private and public according to the place where they encrypt and decrypt.

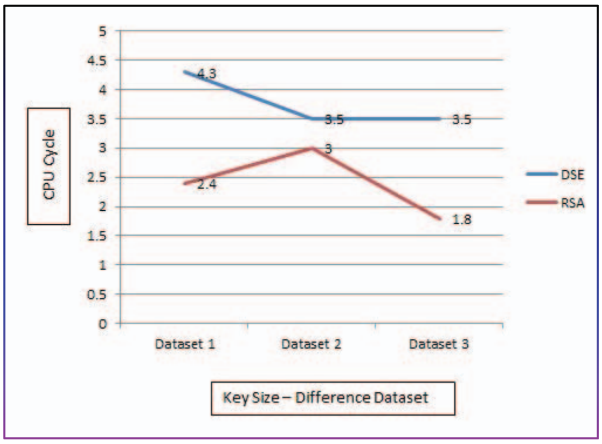

Figure 5.1: DSE Vs RSA Comparison

VI. CONCLUSION

Here the study of symmetric DES and asymmetric key RSA encryption algorithms is done according to different needs. The key used is defined in terms of encryption and decryption either it is same or different. The algorithm used is defined according to its type symmetric or asymmetric. The key length is used according to bit value. The speed is defined in terms of fast or slow. The power consumption takes as low or high. The security is defined as excellent, not secure and least secure. The cost is defined as cheaper or costly. The implementation according to its algorithm used is simple or complex.so it mainly depends on the data and needs of security to that message.

VII. FUTURE WORK

This proposal view presents a detailed study of the popular Encryption Algorithms such as RSA, DES. The use of internet and network is moving more rapidly than other process. So there are more requirements to secure the data passed on various system over modern networks using different services. To provide the security to the network and data various encryption methods are used. In this paper, a survey and analysis on the existing works on the Encryption and decryption techniques has been done[10]. To sum up of this technique, all the techniques are useful for real-time Encryption and also it provide many efficiency of it usage. Each technique is unique in its own way, which might be suitable for numerous applications and has its own merits and demerits of method. According to research done and literature survey,it can be found that DES algorithm is most efficient in terms of speed, time, and throughput and avalanche effect. The cloud security gives by these algorithms can be upgrade level from the original text further, we will use various algorithms to applied on data. Our future analysis will show this concept and a combination of encryption will be applied either sequentially data process or parallel technique, to setup a more secure circumstance for data storage and retrieval of the data.so we can use the cloud security methodology.

REFERENCE

[1] Webber, Glenn, Eamonn Courtney, and Jacqueline Cole-Courtney. "Data encryption and smartcard storing encrypted data." U.S. Patent 9,235,698, issued January 12, 2016.

[2] Gugnani G, Ghrera SP, Gupta PK, Malekian R, Maharaj BT. Implementing DNA Encryption Technique in Web Services to Embed Confidentiality in Cloud. InProceedings of the Second International Conference on Computer and Communication Technologies 2016 (pp. 407-415). Springer India.

[3] A. H. Al-hamami, M. A. Al-hamami and S. H. Hashem, "A Proposed Modifications to Improve the Performance of Blowfish Cryptography Algorithm", First National Information Technology Symposium (NITS 2006) Bridging the Digital Divide: Challenge and Solutions, King Saud University, Riyadh, Kingdom of Saudi Arabia, 5-7 Feb. 2006.

[4] Cochran, William Troy. "Role based encryption without key management system." U.S. Patent 8,995,665, issued March 31, 2015.

[5] Obukhov, Dmitry S., and Zhenchuan Chai. "ENCRYPTION KEY SELECTION." U.S. Patent 20,150,242,640, issued August 27, 2015.

[6] Daemen, Joan, and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[7] Barker, William Curt, and E. B. Barker. Recommendation for the triple data encryption algorithm (TDEA) block cipher. 2012.

[8] Verma, Om Prakash, Ritu Agarwal, Dhiraj Dafouti, and Shobha Tyagi. "Peformance analysis of data encryption algorithms." In Electronics Computer Technology (ICECT), 2011 3rd International Conference on, vol. 5, pp. 399-403. IEEE, 2011.

[9] Singh, Simar Preet, and Raman Maini. "Comparison of data encryption algorithms." International Journal of Computer Science and Communication 2, no. 1 (2011): 125-127.

[10] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 1, pp. 647-651. IEEE, 2012.