ISSN: 2455-2631 © November 2016 IJSDR | Volume 1, Issue 11

Enhancement in Security of Data in Cloud Storage using Key-Exchange and Encryption Standards.

[1]Ravikant K, [2]Umesh Kumar Lilhore

[1] M.Tech Scholar, [2]Asst. Professor
Department Of CSE,
NRI Institute Of Information Science & Technology, Bhopal (MP)

***Abstract*— Nowadays most of the people are using cloud environment for their storage, application support and platform support. Due to having the limited physical storage in PC/ laptops or in mobile phones, users are getting diverted towards the cloud storage. As the habit of cloud is growing day by day, the major concern is the security of data in the cloud. Some of the organizations have given the option to store the encrypted files on the cloud, but another aspect which comes in front of us is the authenticity of the user, whether a valid user is downloading the files from the cloud or not. There are many algorithms which are used to provide the security of the data in the cloud such as DES, TDES, AES for encryption and decryption. Other algorithms for key exchange are Diffie-Hellman, RSA, etc. In this paper we are analyzing different algorithms for the security of data.**

***IndexTerms*— Cloud, Cryptography, RSA, DES, TDES, Diffie-Hellman.**

I. Introduction

Cloud computing environment is a distributed architecture that centralizes the server resources on the available demand computing resources and services. Cloud service provider's offers different platforms for their users and other services such as SaaS, PaaS and IaaS. There are various reasons to move towards the cloud infrastructure as they are required to pay for the resources on the consumption basis.[1]

Software as a Service (SaaS), the Cloud Service Provider (CSP) are very much responsible for executing and maintaining application softwares and other computing resources. The users view the SaaS cloud model as a web based interface between them and the cloud. The applications available on the cloud are provided to the users through the internet and are accessed by the web browser [2]. Examples of SaaS are Zoho, Google Apps.

Platform as a Service (PaaS), the CSP's are also very much responsible for running and maintaining the system software and computing resources. The user can run different applications which require different platforms. Examples are Azure, Google Apps and Aptana cloud.

Infrastructure as a Service (IaaS), the CSP's also provide virtualized computing resources such as network bandwidth, storage and memory. The user can run their applications and platforms with these virtual resources. Example is Dropbox, Amazon EC2.

In this survey we will try to find the security of data through key exchange and cryptographic standards. Encryption is one of the means to guarantee security of sensitive information. Encryption performs various substitutions and transformations on the plain text and transforms into cipher text[3]. Encryption algorithms are classified into two groups: symmetric key (also known as secret key) and asymmetric key(also known as public key) encryption.[4]

A key is a numeric or alpha numeric text or may be a special symbol. The key is used for both encryption and decryption. The strength of encryption relies on the secrecy of the key, length of the key and all together.[5]

II. Detailed Description of Algorithms

A. Diffie-Hellman Key Exchange Algorithm

This key agreement protocol was the first method for establishing a shared secret number over an unsecured communication channel. The sender and receiver agree on a key that two parties can use a symmetric encryption in such a way that a hacker cannot obtain a key.

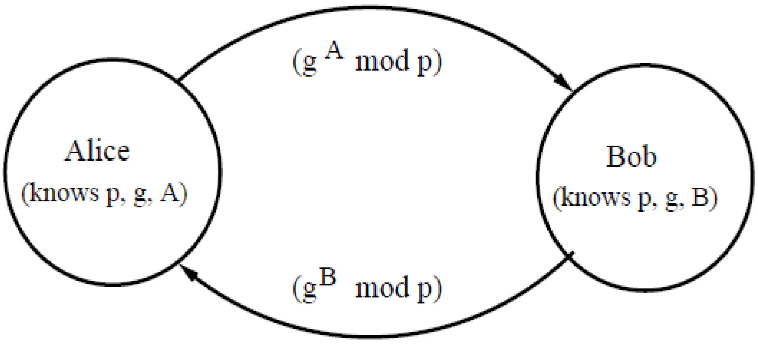


Figure1: Diffie-Hellman Key Exchange Algorithm

Algorithm.

1. Sender and receiver agree on a prime number p and base generator g.
2. Sender chooses a secret number a and sends to the receiver g^a mod p.
3. Receiver chooses a secret number b and sends to sender g^b mod p.
4. Sender computes [(g^b mod p) mod p].
5. Receiver computes [(g^a mod p) mod p].

Both sender and receiver can use this key which is calculated at step 4 and 5.

B. RSA (Rivest Shamir and Adleman)

This algorithm is an asymmetric cryptographic algorithm used for encryption and decryption. Asymmetric means it has two keys, one is public key and other is a private key which is known only to the user.

Algorithm

1. Generate two large random primes, p and q, of approximately equal size such that their product n = pq is of the required bit length.
2. Compute n = pq and (phi) φ = (p-1)(q-1).
3. Choose an integer e, 1 < e < phi, such that gcd(e, phi) = 1.
4. Compute the secret exponent d, 1 < d < phi, such that ed ≡ 1 (mod phi).

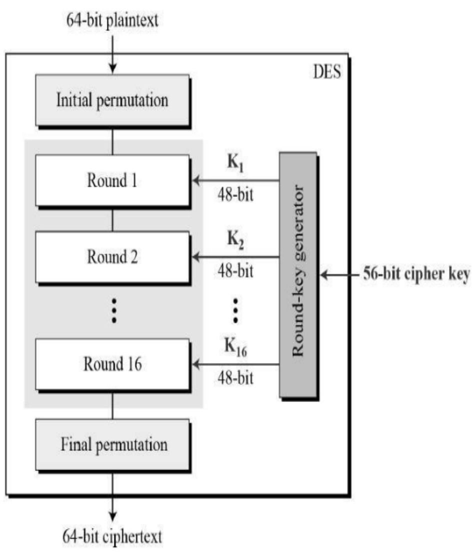
- The public key is (n, e) and the private key (d, p, q). Keep all the values d, p, q and phi secret

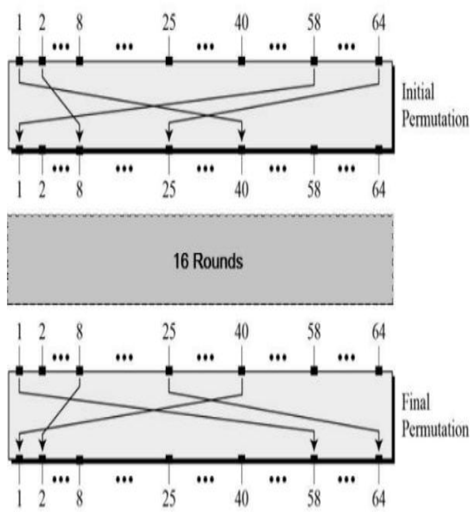
n is known as the modulus.

- e is known as the public exponent or encryption exponent or just the exponent.
- d is known as the secret exponent or decryption exponent.

C. DES (Data Encryption Standards)

DES is a symmetric key block cipher which is implemented in feistel cipher. The block size is 64-bits and it has 16 rounds. The DES has an effective key length of 56 bits, as 8 bits are not used for encryption algorithm.





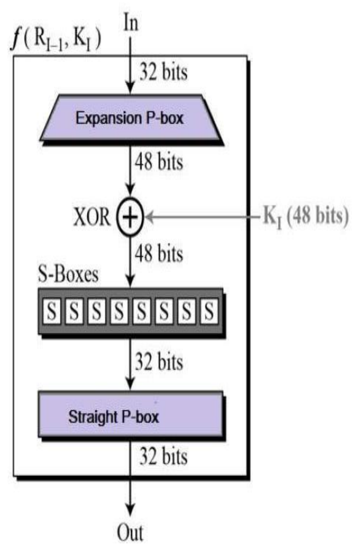


Figure1: DES Structure Figure2: Initial & Final permutation Figure3: Round Function

D. TDES (Triple DES)

The TDES is a symmetric key block cipher, which works on the principle of DES algorithm. It applies the DES three times to the each block. TDES uses 64 bit block cipher and performs 48 processing rounds. In TDES three times iteration is performed to increase the encryption levels and security.[6]

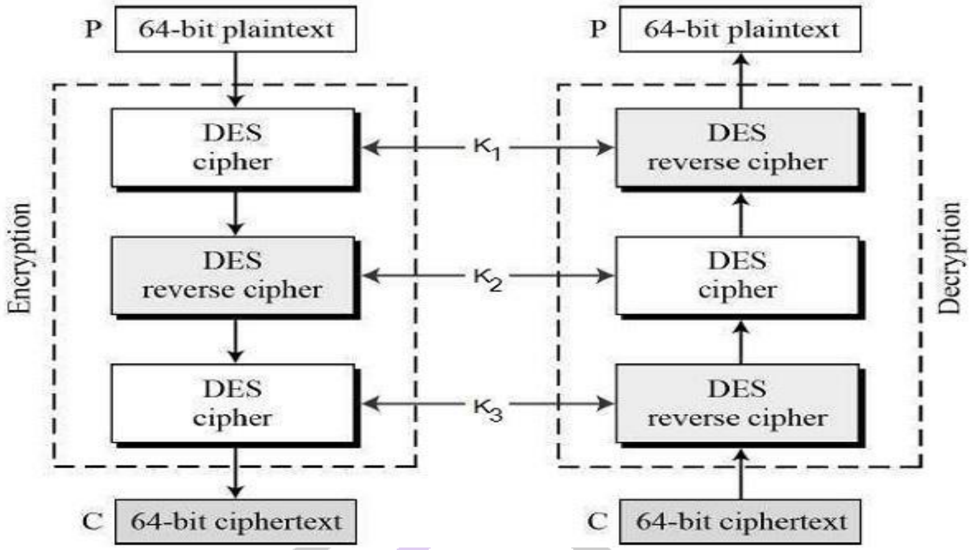


Figure4: Triple DES

Algorithm.

1. Encrypt the plain text using single DES with key K1.
2. Now decrypt the output of step1 using single DES key K2.
3. Finally encrypt the output of step2 using single DES with Key K3.
4. The output of step3 is the cipher text.
5. Decryption of a cipher text is a reverse process. User first decrypt using K3, then encrypt with K2 and finally decrypt with K1.

III. LITERATURE REVIEW

To enhance the security of data while storage in cloud environment. A framework is developed by Deepika Verma and Karan Mahajan [6] which includes role based access control, encryption and key verification. In this methodology user login to his account and encrypt the data using some encryption algorithm and stores the encrypted data into the cloud. Now whenever user wants to access his data, he downloads the data and decrypts the data using a key-exchange algorithm for verification. The key is stored in the cloud and user decrypts the data with his/her private key which is securely kept by the user. Before analyzing the concept given by the author, let us discuss about some other algorithms and their decryption times.

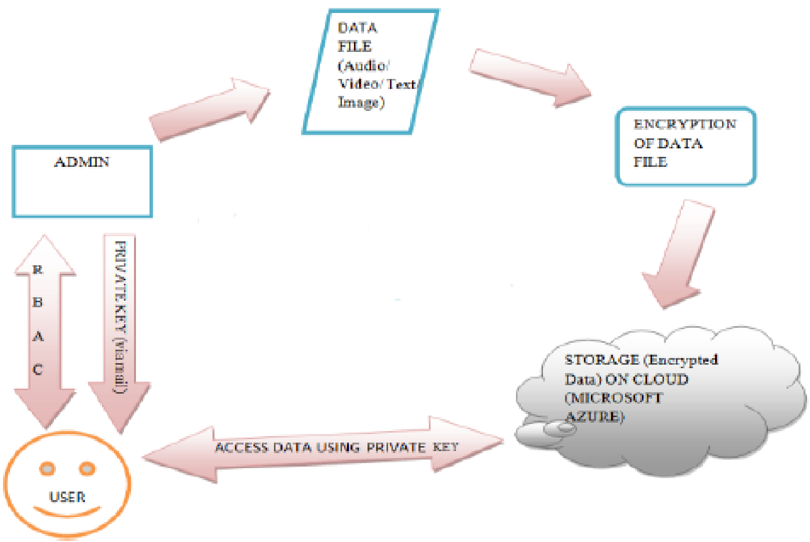


Figure5: Survey Methodology

Method-1:

When only cryptographic algorithms were used for encryption and decryption, such as RSA (Rivest, Shamir and Adleman) and DES (Data Encryption Standards). The advantage of this method is that the execution time of encryption and decryption was very less.

Advantage

RSA

- It is secure because it is difficult to factorize the number. More larger the number more is the security.

DES

- DES uses 64-bit block for cryptography.

Disadvantage

RSA

- Complexity of key which makes the process slow.

DES

- The purpose of initial and final permutations are not clear.

The main drawback of this method is that the user is not verified before accessing the data from the cloud. There is no authentication of user. Now let us analyze the decryption time for various data.

Table 1

Decryption Time of single algorithms (without combining with other key exchange algorithms)

Data Size (byte)	RSA (Av) in ms	DES (Av) in ms	No. of Iterations
643	38.2	12.8	5
2342	34.0	7.8	5
4921	34.6	9.0	5
14763	42.2	15.6	5
29526	34.6	41.2	5

Method-2:

Taking the security as a major factor, author analyzed that the key exchange algorithms can be used for enhancing the more security of data access. User tries to decrypt the data which is downloaded from the cloud but it is extremely important to authenticate the user. User enter the private key and proves is authenticity. Now Diffie-Hellman key exchange algorithm is implemented with cryptographic algorithms for enhancing the security and user authenticity.

Advantage

- It allows two parties to establish over an insecure communication channel. The two parties only know the shared key.

Disadvantage

- The main drawback of this method is the problem of large factoring numbers.

- Table 2
- Decryption Time of algorithms combined with Diffie-Hellman Key Exchange algorithm

Data Size (byte)	Diffie-Hellman (Av) in ms	Diffie-Hellman+ RSA (Av) in ms	Diffie-Hellman+ DES (Av) in ms	No. of Iterations
643	15	53.2	27.8	5
2342	15	49.2	22.8	5
4921	15	49.6	24.0	5
14763	15	57.2	30.6	5
29526	15	49.6	56.2	5

Method-3:

This method replaces the DES algorithm with another higher version of DES, ie- TDES (Triple DES). TDES is implemented by cascading three instance of DES with distinct keys. 3DES is secure upto 2^{112}, which is very high security standard but is slow in software.

Table 3

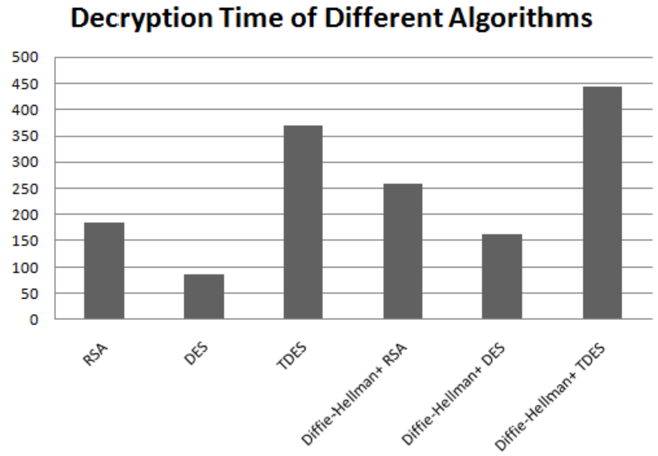
Decryption Time of TDES algorithms combined with Diffie-Hellman Key Exchange algorithm

Data Size (byte)	Diffie-Hellman (Av) in ms	TDES (Av) in ms	Diffie-Hellman+ TDES (Av) in ms	No. of Iterations
643	15	36.8	51.8	5
2342	15	53.6	68.6	5

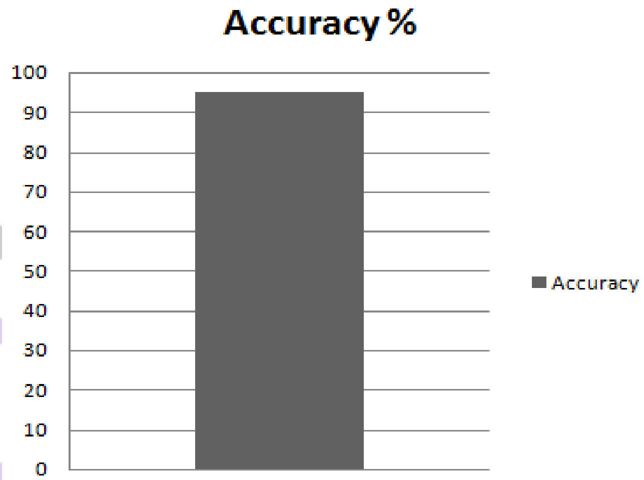
4921	15	53.8	68.8	5
14763	15	86.6	101.6	5
29526	15	138.2	153.2	5

IV. RESULTS OBTAINED IN SURVEY

In the table 3, we have taken different algorithms and some combination with key exchange algorithms to make hybrid algorithm. Therefore we found that the decryption time of single TDES is much higher than DES and RSA but TDES has greater security standards. When it is combined with a key exchange algorithm Diffie-Hellman, again TDES has higher decryption time.



Graph 1



Graph 2

The accuracy of this hybrid algorithm is calculated by checking the equality between the total plain text encrypted in bytes and the total cipher text decrypted accurately. Accuracy calculated is around 95%.

V. CONCLUSION AND FUTURE SCOPE

As in this survey, we found the combination of two algorithms for key exchange and cryptography. The hybrid algorithms are enhanced with high security but it takes more time to decrypt the data. In our proposed algorithm we will try to combine other advance key exchange and cryptographic algorithms and try to reduce time consumption for decryption.

REFERENCES

[1] Rabi Prasad, Manas Rajan, Suresh Chandra" Cloud computing security issues and research challenges" Internation Journal Of Computer Science And Information Technology Secirity," Vol 1, No2 Dec 2011.
[2] Ahmed E Youseef "Exploring Cloud computing services and applications"Journal Of Emerging Trends In Computing And Information Science" Vol 3, No6 July 2012.
[3] Gurpreet Singh and Supriya "A Study of Encryption Algorithms(RSA, DES, 3DES and AES) for Information Security" International Journal Of Computer Applications" Vol 67, April 2013.
[4] E. Thambiraja, G. Ramesh and Dr. R. Umarani "A Survey On Most Common Encryption Techniques" International Journal Of Advance Research In Computer Science And Software Engineering" Vol 2, July 2012.
[5] William Stallings."Cryptography & Network Security: Principles and Practices" Pearson Education.
[6] Deepika Verma And Karan Mahajan "To Enhance The Data Security In Cloud Computing Using Combination Of Encryption Algorithms" International Journal Of Advances In Science And Technology" Vol 2,Issue 4 Dec 2014.
[7] Pranita P. Khairnar and Prof. V.S. Ubale, "Cloud Computing Security Issues And Challenges", International Refereed Journal of Engineering and Science (IRJES), Volume 2, Issue 2, PP.01-13, February 2013
[8] Mandeep Kaur and Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", International Journal of Communication and Computer Technologies, Volume 01, Issue 03, pp.56-59, January 2013.
[9] K. S. Suresh and Prof K. V. Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 2, Issue 10, pp.110-114, October 2012.