Comparison of DES and RSA Algorithm for Security purpose in Cloud Computing

[1] Miss Arpita Shukla, [2] Dr. Pratima Gautam, [3] Dr. Rajendra Gupta
[1]Research Scholar, [2]Dean of Computer Science and Information Technology, [3]HOD of Computer Science and Information
[1]Computer Science and Information Technology, [2]Computer Science and Information Technology
[1]Rabindranath Tagore University, Bhopal, India

Abstract

Cloud computing has come to be on the top of any list of topics in the fields of computer because of its cost effectiveness. Storage and maintenance of large amount of data used to be a nightmare of the end users, but the advent of cloud computing gave them breathers because of its third party computing capabilities, thereby cutting the cost of infrastructure and man power. Number of users stores their data on Cloud. Data storage security is known as the security of data on the storage media. Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud [6]. For this purpose cryptography algorithms are proposed. The use of relevant algorithm deals with the level of data safety in cloud because data security in cloud computing is a major issue as the data centers are located worldwide. Authentication is the essential procedure to fix the cloud data in a secured manner. Data security is a important issue of cloud computing. Thus, the need to ensure and confirm the safety of information that being transfer between the users and the cloud became more significant. Many security and authentication techniques(known as security) have been proposed to secure the exchanged data. These techniques aim to keep the authentication, privacy and reliability levels of data [7].

Keywords- Cloud Computing, DES, RSA, Security, Cryptography, Encryption, Decryption

I. Introduction-

In the modern world of computing and e-governance both in the private and public sectors including various governmental departments and organizations, cloud computing has become a keyword. Cloud computing means storing once data in a rented server thereby saving on the infrastructure cost and the cost of man power. Although the future of computer lies in cloud computing, a major concern is the security of user data since it is kept in an open environment. Security of the data is of paramount importance because of ever growing use of data and the tremendous competition brewing among the software and hardware manufacturers and users. Therefore, there is a major concern of data security and privacy which is impeding the expected growth of the field of cloud computing. Since many users upload their data to the same cloud server there is danger of pilferage of data. So computer based security measures should emphasis on user authorization and authentication.

When the client uploads his data to the cloud server, it should be with proper security measures to ensure that the access to his data will be restricted to the authorized access. In other words a cloud space client should be cent-percent assured as to the security of his data and the related privacy policies and legalities.

II. Problem Statement

Cloud computing technology has various policies issues and threats, in which include privacy, segregation, storage, reliability, security, capacity and more. But most important in this to concern is security and how service provider assures it to maintain. The future of computing lies in cloud computing. But as the demand for cloud computing Client of cloud computing increases, so is the security threat for client-data. Therefore along with the space for cloud computing ensuring data security is very significant. So more complex methods are to be advised for ensuring data security which can take the clients into confidence.

III. Research Methodology

This research methodology work to comparison between DES Algorithm and RSA Algorithm, which cryptography techniques are best for security. Because security becomes big issue when any one stores its important information to a platform which is not directly controlled by the user and which is far away. We use DES an RSA algorithm for cryptography techniques. DES uses single key (secret key) for both encryption and decryption and RSA is used to block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Also RSA cryptography algorithm in this research to convert plain text to cipher text then that code is converted to cipher text and follow this procedure security level becomes very high.

IV. Related Work

T. Ramaporkalai et al. discussed that people are saved their personal and important data to clouds, so it becomes a major issue to store that data safely. Many algorithms are exist for the data security like Triple DES, DES, and AES. These are symmetric key algorithms in which a single key is used for encryption and decryption whereas asymmetric key algorithm are RSA, Diffie-Hellman Key Exchange and Homomorphism equations, in this algorithms two different keys are used for encryption and decryption [7].

P.Pushpa , Dr. G.N.K. Suresh Babuet et al. There are many security algorithms, but security of all these algorithms can be broken by anyone. So it is necessary to make security of cloud environment more strong. After reviewing all the algorithms, the author suggests that no one algorithm is giving better security. Every algorithm has certain advantages and disadvantages so that we have to combine the best features of all algorithms and give the optimized solution [3].

Nasarul Islam. K. V, Mohamed Riyas. K.V Comparison of secret key and public key based DES and RSA algorithms, it clears that RSA solves the problem of the key agreement and key exchange problem generated in secret key cryptography. But it does not solve all the security infrastructure .So DES is used. RSA and DES differ from each other in certain features [1].

R. Gowthami Saranya, A. Kousalya proposed Data Security has become the most important issue in cloud computing security. Since, Data and Information should not be leaked to the third party user an efficient data security algorithms should be implemented. According to author various security algorithms in cloud using cryptographic techniques. Different algorithms are use different protection techniques but they all are liable to different situations. So the single security algorithms can't be trusted [5].

Parsi Kalpana, Sudha Singaraju, Thus, in our proposed work, only the authorized user can access the data. Even if some unauthorized user gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it. Hence forth, data security is provided by implementing RSA algorithm [4].

V. Proposed Work

❖ DES

The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). It uses single key (secret key) for both encryption and decryption. It operates on 64-bit blocks of data with 56 bits key. The round key size is 48 bits. Entire plaintext is divided into blocks of 64bit size; last block is padded if necessary. Multiple permutations and substitutions are used throughout in order to increase the difficulty of performing a cryptanalysis on the cipher. DES algorithm

consists of two permutations (P-boxes) and sixteen feistel rounds [1]. Block Cipher which is designed to encrypt and decrypt blocks of data consisting of 64 bits by using a 64-bit key. Since that time, so many attacks and methods have weaknesses of DES, which made it an insecure block cipher [6].

DES Encryption Algorithm:

- Plaintext is broken into blocks of length 64 bits. Encryption is blockwise.
- A message block is first gone through an initial permutation IP, then divided into two parts L0,where L0 is the left part of 32 bits and R0 is the right part of the 32 bits.
- Round i has input Li-1,Ri-1 and output Li,Ri

  $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_i\text{-}1,K_i)$

  and K_i is the subkey for the 'i'th where $1 \leq i \leq 16$

  $L_1 = R_0$, $R_1 = L_0 \oplus f(R_0,K_1)$

  $L_2 = R_1$, $R_2 = L_1 \oplus f(R_1,K_2)$

  $L_3 = R_2$, $R_3 = L_2 \oplus f(R_2,K_3)$

  ....

  ....

  ....

  $L_{16} = R_{15}$, $R_{16} = L_{15} \oplus f(R_{15},K_{16})$
- After round 16,L_{16} and R_{16} are swapped, so that the decryption algorithm has the same structure as the encryption algorithm.
- Finally, the block is gone through the inverse the permutation IP^{-1} and then output
- One round of DES in very simple way during encryption.

DES Decryption Algorithm

- Observation: In encryption, we have

  $L_i = R_{i-1}, R_i = R_i = L_{i-1} \oplus f(R_{i-1},K_i)$

- and K_i is the sub key for the 'i'th round. Hence

  $R_{i-1} = L_i, L_{i-1} = R_i \oplus f(L_i,K_i)$ for each 'i'

- Due to swap operation after the 16th round encryption, the output of encryption is $IP^{-1}(R_{16},L_{16})$

- Equation (1) as follows:

  $R_{15} = L_{16}$, $L_{15} = R_{16} \oplus f(L_{16},K_{16})$

  $R_{14} = L_{15}$, $L_{14} = R_{15} \oplus f(L_{15},K_{15})$

  $R_{13} = L_{14}$, $L_{13} = R_{14} \oplus f(L_{14},K_{14})$

  ....

  ....

  ....

  $R_1 = L_2$, $L_1 = R_2 \oplus f(L_2,K_2)$

- If we give $IP^{-1}(R_{16},L_{16})$ as the input for the same algorithm with round sub keys($K_{16},K_{15},.....K_1$),then the output is $IP^{-1}(L_0,R_0)$,the original message block

- Decryption is performed by using the same algorithm, except the K_{16} is used as first round,K_{15} in the second, and so on, with K_1 used in the 16th round

- One round of DES in very simple way during decryption [8].

❖ RSA

RSA is widely used Public-Key algorithm. RSA known for name Ron Rivest, Adi Shamir and Len Adleman, who described it in 1977 publicly. RSA algorithm use to encryption of data to provide security for concerned user who can access it. By secured the data, security algorithm not allowing unauthorized access to it. RSA is used to block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, Cloud service provider done encryption process and decryption process is done by the Cloud user or consumer. When data is encrypted with the Public Key, it can be decrypted use the corresponding only with Private-Key [3]. It is first public key cryptosystems used for secure data transmission. In this algorithm the encryption key is public & the decryption key is private. It is asymmetric cryptography algorithm which means it use two different keys [7].

Concept- RSA is based on concept that is difficult to factorize a large integer. The public key is combination of two numbers one is multiplication of two large prime numbers and private key is also derived from same two prime numbers

Plaintext- It is the original message

Cipher text- It is the disguised message

Encryption- It is a security mechanism in which the plaintext are transformed by the encryption process into cipher text.

Decryption- A procedure to convert cipher text back into plaintext.

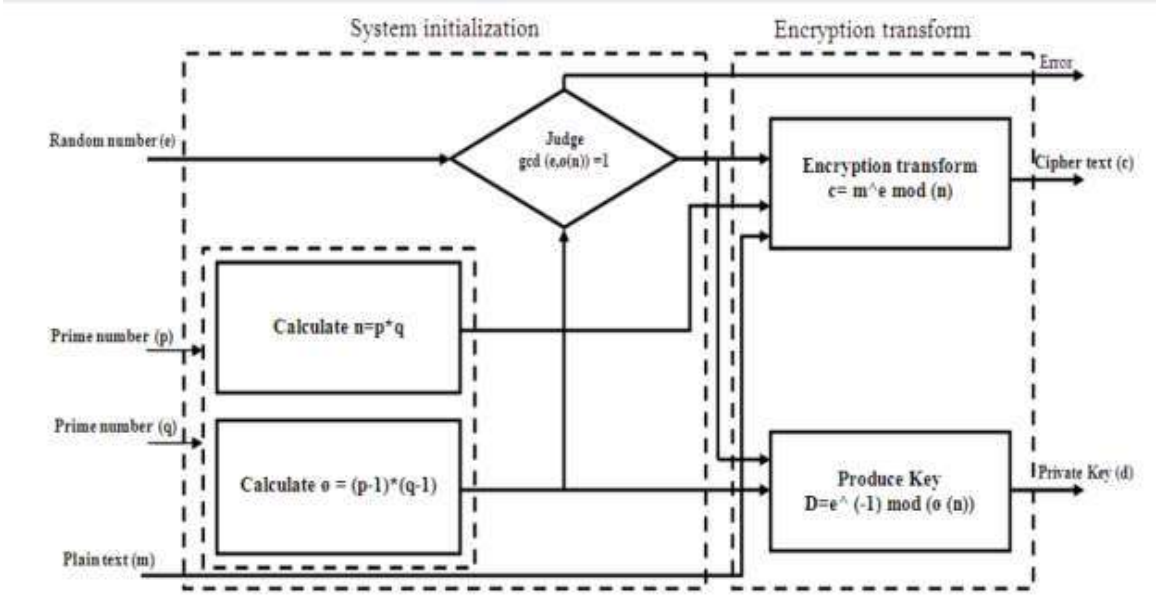

Fig. 1: Block diagram of RSA algorithm

Algorithm- Three steps are follow

- key generation
- key distribution
- key decryption

Key generation

Step-1: Generate- Two prime numbers P and Q

Step-2: Let N = P*Q

Step-3: Let $\phi(N) = (P-1)(Q-1)$

Step-4: Choose a small number e, co-prime to $\phi(N)$, with GCD $(\phi(N),E) = 1$ $(1<E<\phi(N))$

Step-5: Find D, such that $D*E \bmod \phi(N)=1$ publish E & N as the public key.

Keep D and N as the secret key

Encryption

Cipher= $(\text{message})^E \bmod N$

Decryption

Message = $(\text{cipher})^D \bmod N$

X mod Y means the remainder of x divided by y

Example of RSA

Step 1: select primes: P = 3 and Q = 7;

Step 2: compute N = P*Q = 3*7 = 21;

Step 3: compute $\phi(N) = (P-1)(Q-1) = 2*6 = 12$;

Step 4: select gcd(E,12) = 1, we choose E = 5;

Step 5: compute D, DE = 1 mod 12 and D<12, so D = 5;

Step 6: **Encryption** Cipher = $(\text{message})^E \bmod N$, cipher = $(11)^5 \bmod 21 = 2$

Decryption Message = $(\text{cipher})^D \bmod N$, message = $(2)^5 \bmod 21 = 11$

Table:1 Comparisons of DES and RSA in Cloud Environment.[2]

FEATURES	**DES**	**RSA**
Key size	56- bits	Based on No. of bit in N=p*q
Initial vector size	64 bits	1024 bits
Type of key	Same key is used to encrypt and decrypt data.	Public key is used for encryption and private key is used for decryption.
Type of Cipher	Symmetric Block cipher	Asymmetric i.e. two keys involved encryption and decryption done with different keys.

Number of Rounds	16	1
Block size used	64-bits	Variable
Security rate	Fair	Secure for both providers and user.
Attacks	Brute Force Attack	Chosen plaintext attack, chosen Cipher text attack
Authentication Type	Message authentication used	Robust authentication implemented

VI. Result and Discussion

Many encryption algorithms are in use nowadays in Cloud computing environment to protect user data from various attacks as described in previous sections. Here I compare DES and RSA for security in cloud computing. The selected algorithms DES and RSA are discussed in cloud environment. As DES is secret key (single key) based algorithm suffers from key distribution and key agreement problems. But RSA use concept of private key and public key to achieve encryption and decryption process. Comparison result showed that RSA has better performance than DES. From the Comparison results, I evaluated that throughput of RSA algorithm is much better than the throughput of DES algorithm.

VII. Conclusion and Future Work

Cloud computing is world emerging, next generation technology in the field of information technology. It has numerous advantages but some challenges still exist in this technology. Security is the most challenging issue in this technology. In this paper we compare DES and RSA encryption algorithms to overcome this security issue. To provide the security using over the network and data different encryption methods are used. In this paper, existing works on the Encryption techniques has been done. To sum up, both techniques are useful for real-time Encryption. Both techniques 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 found that RSA algorithm is most efficient in terms of Security, Efficacy, Reliability, Throughput and avalanche effect. The Security provided by this algorithm can be enhanced further, if more than one algorithm is applied to data.

Our future work will explore this concept and uses of algorithm will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval. Cloud computing expand several new trends, like using software that are not present on your computer, accessing data from anywhere. One of the big benefits of cloud computing is virtualization, but we can use cloud computing service properly only if it provides reliable security. Cloud computing is commonly used because it provides much storage space to its user, so it becomes necessary to provide security to that data. There are many security algorithms, but security of all these algorithms can be broken by any specialized person. So it is very necessary to make security of cloud more strong [7].

Refrences :

1) Nasarul Islam.K.V, Mohamed Riyas.K.V, "Analysis of Various Encryption Algorithms in Cloud Computing", International Journal of Computer Science and Mobile Computing, Vol.6 Issue.7, July- 2017.
2) Nidhi Grover, "A Comparative Study of Various Data Encryption Techniques in Cloud Computing", International Journal of Computer Science And Technology, IJCST Vol. 5, Issue 1, Jan - March 2014.
3) P.Pushpa, Dr. G.N.K.Suresh Babu, "A Review Of Security Algorithms In Cloud Computing Environment", Tecnihnical esearch Organization India, Volume-4, Issue-8, 2017.
4) Parsi Kalpana, Sudha Singaraju, "Data Security in Cloud Computing using RSA Algorithm", International Journal of Research in Computer and Communication technology,IJRCCT, Vol 1, Issue 4, September 2012.

5) R.Gowthami Saranya, A.Kousalya, "A Comparative Analysis of Security AlgorithmsUsing Cryptographic Techniques in Cloud Computing", International Journal of Computer Science and Information Technologies, IJCSIT Vol. 8 (2) , 2017.
6) Randeep Kaur ,Supriya Kinger, "Analysis of Security Algorithms in Cloud Computing", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 3, March 2014.
7) T.Ramaporkalai, "Security Algorithms in Cloud Computing" , International Journal of Computer Science Trends and Technology (IJCST) – Volume 5 Issue 2, Mar – Apr 2017.
8) http://www.umsl.edu/~siegelj/information_theory/projects/des.netau.net/Dataencryptionalgorithm.html