Security of Data Transmission in Cloud Computing

[1]Zeyad Halabi, [2]Faisal Babtain, [3]Mohammed Saif
[1,2,3]Dept. of Computer Science and Engineering, Taibah University, Saudi Arabia

Abstract
Cloud computing is a very popular and interesting technology today; a lot of people are using cloud services directly or indirectly like e-mail, Facebook or ICloud etc. These are some application using cloud computing to get access them anywhere at any time just you need a connection with internet. Also, cloud computing have the ability to store any kind of data, and users can access and store their data with low cost, high features, and good services provided. During that flexibility, everyone now using cloud to transferring there data. For storing data via cloud the user has to send the data to the service provider who will managing and storing data. So, it is very important for companies to secure that data. The data will be secured if its integrity, availability, and confidentiality is present. For securing data there are many algorithms are developed. This paper discusses the popular kinds of cryptography of algorithms.

Keywords
Cloud computing, Cryptography, Encryption, Decryption, Cipher Text, Plain text, DES, TDES, AES, RSA, Homomorphic.

I. Introduction

Cloud services are a group of servers and data centers that are exist in several places, and these servers and data centers are responsible for producing on demand service to its users on accepted interfaces. The service produced by cloud is not exist on user's hardware. The user has to access to its services by using the internet connection and subscribing with services provider. The biggest benefit when using cloud computing is that the user does not need to be exist on the same location where hardware, software, and storage are physically presented, Cloud service makes that possible to storing and accessing your data from any place and anytime without worrying about monitoring and maintenance of software, hardware and storage space. All these services are produced to user at low cost. The user has to buy a storage space as what he needs, with all these flexibility everyone is using cloud to transferring the data. Security become a big issue, because a lot of us storing there important information in a place that is not directly controlled by them which is also too far away from them[1]. While sending the data and during storing process, data is expose to threat because any unauthorized user can access to it and modify it. So, that data should be secured. The data will be secured if it applying three conditions which are availability, integrity, and confidentiality.

Availability is a process to ensure that the user can access to its information anytime and from any network. Integrity means data received by receiver should be in the same form the sender sends it. Integrity is the process that preventing modification from unauthorized user. Confidentiality is a process that the data is understandable only by receiver and for all others it will be meaningless. It prevents the unauthorized to detect of sensitive information. It applied by cryptography.

Cryptography is a technique that converting data into form that unreadable during storage and transmission to look meaningless. The unreadable form of data is known as cipher text. But when data is arriving to the receiver, it will be in its original form which is called plain text.

Converting the plain text to cipher text is known as encryption, and returned to prevent form is called decryption. Encryption applied at sender's phase where decryption applied at receiver's phase.

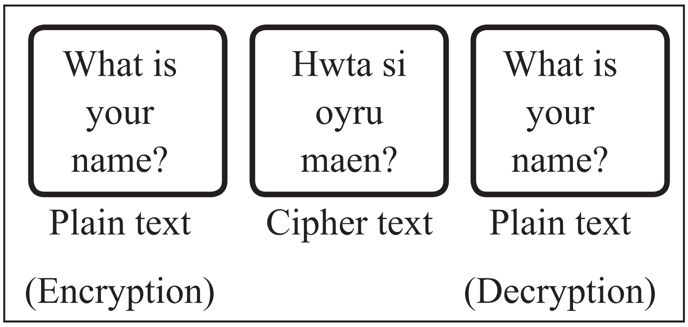

Fig. 1: The Process of Encryption and Decryption

The cryptography algorithms have three types (Symmetric, Asymmetric, and Hashing).

In hashing the length of signature is created by help from algorithms or function for encryption the data. Every message contains a different hash value, but the hash has one impediment. Once data is encrypted, it can't be decrypted. This statement is limited the hashing in removing by symmetric and asymmetric algorithms. Symmetric algorithm is called a "Secret Key Encryption" in symmetric, which only one key used to encrypt and decrypt, and private key, where asymmetric algorithm has the public and private keys and used to encryption and decryption, asymmetric algorithm is also known as "Public Key Encryption" [2].

II. Related Work

Research paper: A Study of Encryption Algorithms AES, DES and RSA for Security [3].

Research paper: A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique [4].

A. Existing Algorithms

There is many organizations and people store the data on cloud servers and the data is also accessible by some persons, so that is important to securing data from aliens. There are many algorithms have been established to provide security to the cloud and mention some of popular algorithms used: -

B. Data Encryption Standard (DES)

The Data Encryption Standard is very commonly used symmetric algorithm. It was established by IBM in 1974, but now many methods define and prove that the (DES) not secure [2]. In this algorithm the block cipher is about 64 bits [5] and key used is about 56 bits out of 64 bit of key is used the rest which is 8 bits. Also, in block cipher it encrypts the block of data which contain of plain text that combination of confusion and diffusion to make it then this cipher block need to pass 16 round, but before passing through these rounds the 64 bits of data is divided to 32 bits. After that, F-function (Festal function) is applied. it contains of permutation, substitution, and key mixing. The output of F-function is combined with another half of the data using XOR that alternate crossing of data is done, after it did 16 rounds cipher text provided encryption of data is done. for decrypt the data reverse is done. The impediment of this algorithm is that the key used in DES is too small and it's not secure enough so that it can be broken easily and DES working slowly on software and fast on hardware.

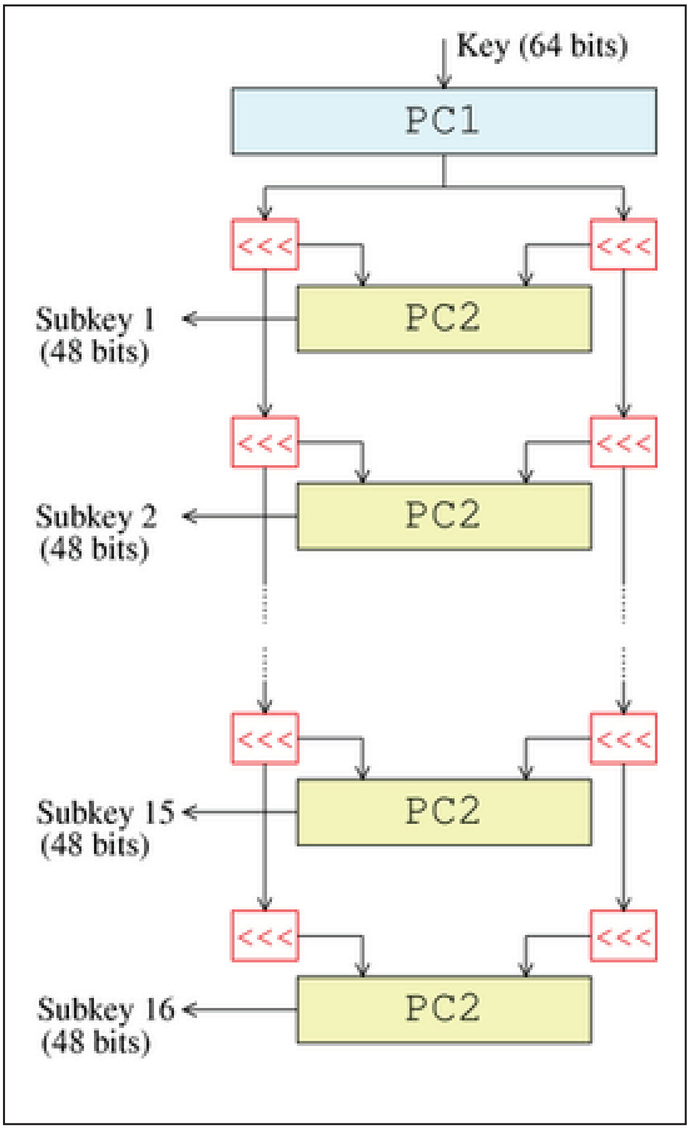

Fig. 2: DES Example

C. Advance Encryption Algorithm (AES)

the Advance Encryption algorithm is known as Rijndael. In AES different size of key used 256, 192 or 128 bits, it depends on number of cycle it uses [6]. For 14 cycles 256-bit key, 12 cycles 192 bit and 10 cycles 128-bit key is used. AES working on 4x4 matrixes. AES contains of key expansion, final, and initial round. Initial round contains of Add Key, Sub Bytes, Shift Rows, Mix Columns, and Add Round Key. Final round contains of same functions as initial round except mix columns. AES working fast on software and hardware.

D. Triple DES (TDES)

Triple Data Encryption Standard is updated version of DES. In TDES the key size increased to 168 bits the security of data, the main different between TDES and DES is that the number of keys on TDES more than on DES [7]. In TDES there are three different keys are run on cipher block.

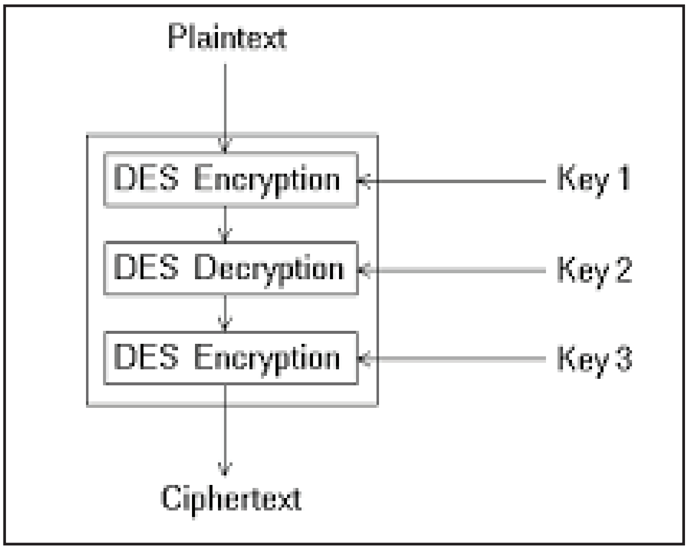

Fig. 3: TDES Example

E. Homomorphic Encryption

Homomorphic encryption applied asymmetric algorithm that two different keys are used to encryption and decryption. Public and private key [8]. The mathematics homomorphic conversion of one set of data to another without losing their relation. In homomorphic complex functions are used to encrypt the data but reverse operation is used for decryption.

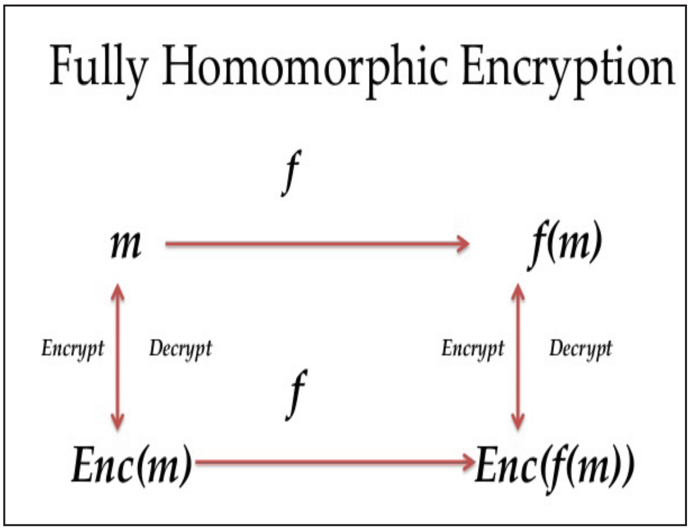

Fig. 4: Fully Homomorphic Encryption

F. RSA

RSA created by Ranold Fivest, Adi Shamir and Leonard Adleman in 1977 [9]. RSA is an asymmetric algorithm. The Functions of RSA are generate two large numbers and multiplied it. Then, it calculates the modulus of number that is generated to used in public and private key [10]. The numbers that used for multiplication-one is public and the second is private. The Steps of RSA algorithm are: -

- Convert large message into small number of blocks that each block represents same range.
- By improve the power of module in encryption the message.
- For decrypt the message increases other powers in module.

III. Conclusion

Cloud computing is very useful services for people and organizations. Most of people are used cloud computing on different ways, due to its flexibility. People are transferring their data by using cloud computing. Cloud services is very successful for organizations because it can store large amount of data. The cloud can provide that space to its user and allows them to access their data anytime and from anywhere easily. As users are saving their sensitive information to clouds, it becomes a huge issue to keep their data secure. There are many algorithms developed for data security such as DES, AES, and TDES. These are symmetric algorithms in which one key is used to encryption and decryption, where RSA Key Exchange and Homomorphic is asymmetric, which two keys are used to encrypt and decrypt data. These algorithms are unsecure, it needs to improve the security of the algorithms.

IV. Future Scope

Cloud computing create new domain like using some software without putting them on your computer, and accessing data become very flexible from anywhere. Virtualization cloud computing is the most benefit, but trusted security that is what makes users using cloud services. Also, cloud computing used because it provides a huge space to its user, so that security is too necessary for keeping data safely. There are a lot of security algorithms, but all of these algorithms can be breach by some people. So that its very necessary to having a good security to cloud computing.

References

[1] Alexa Huth, James Cebula,"The Basics of Cloud Computing", United States Computer Emergency Readiness Team. 2011.

[2] Jawahar Thakur, Nagesh Kumar,"DES, AES, Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis", International Journal of Emerging Technologies and Advanced Engineering (IJETAE), Vol. 1, Issue 2, 2011.

[3] Dr. Prerna Mahajan, Abhishek Sachdeva,"A Study of Encryption Algorithms AES, DES and RSA for Security".

[4] B.Padmavathi, S. Ranjitha Kumari,"A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique.

[5] Neha Jain, Gurpreet Kaur,"Implementing DES Algorithm in Cloud for Data Security", VSRD International Journal of CS & IT, Vol. 2 Issue 4, pp. 316-321, 2012.

[6] Rachna Jain, Ankur Aggarwal,"Cloud Computing Security Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering", Vol. 4, Issue 1, 2014.

[7] Manzoor Hussain Dar, Pardeep Mittal, Vinod Kumar,"A Comparative Study of Cryptographic Algorithms", International Journal of Computer Science and Network", Vol. 3, Issue 3, 2014.

[8] Maha TEBAA, Said EL HAJJI, Abdellatif EL GHAJI, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering. Vol. 1, London U.K, 2012.

[9] B.Persis Urbana Ivy, Purshotam Mandiwa, Mukesh Kumar,"A Modified RSA Cryptosystem Based on 'n' Prime Number", International Journal of Engineering and Computer Science, Vol. 1, Issue 2, 2012.

[10] Shakeeba S. Khan, Prof. R.R. Tuteja,"Security in Cloud Computin Using Cryptographic Algorithms", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, 2015.