IJASRM International Journal of Advanced Scientific Research and Management, Volume 4 Issue 1, Jan 2019
www.ijasrm.com
ISSN 2455-6378

A study on Role and Applications of Cryptography Techniques in Cloud Computing (Cloud Cryptography)

Waseem Akram

Department of Computer Applications,Government Degree College Mendhar, Mendhar, Jammu and Kashmir 185211, India

Abstract

Cloud Computing refers to controlling, arranging, and getting to the equipment and programming assets remotely. It offers online data storage, infrastructure, and applications. Cloud Computing gives customers a virtual computing environment on which they can store information and run applications. But, Cloud computing has presented security challenges since cloud administrators store and handles customer information outside of the scope of customers. As virtualization becomes the main aspects of Cloud Computing But we can use it only if it provides reliable protection and security.

Cryptography is the art of achieving security by providing different encryption algorithms to protect or secure the cloud data. Various encryption techniques of cryptography are used in Cloud to secure data that will be used or stored in the cloud. It enables clients to safely get to shared cloud administrations, as any information that is facilitated by cloud suppliers is secured with encryption. Cryptography in the cloud secures sensitive data without delaying information exchange.

Cryptography in the cloud allows for securing critical data beyond our corporate IT environment, where that data is no longer under our control[1]. In the cloud, we don't have any such mechanism which provides actual and physical control over the storage of information, so the only way we can ensure that the information spreading through cloud is protected, encrypted and stored cryptographically by using various cryptographic techniques and algorithms.

Therefore, in this paper different cryptography aspects that create a threat to cloud computing are reviewed. This paper is a survey of specific security issues brought by the use of cryptography in a cloud computing system and how to implement data security solutions that provide reliable security and protection of sensitive data, including cloud data protection through encryption and cryptographic key management.

Keywords: *Cloud Computing, Cryptography, Encryption, Virtualization, Algorithm.*

1 Introduction:

Cloud computing is an important distributed computing model that is driven by economies of scale. It combined a set of abstract, virtualized, dynamically-scalable, and managed resources, such as computing power, storage, platforms, and services. Customers or clients can access to resources over the Internet using terminals, particularly mobile terminals. Cloud architectures are developed in on-demand fashion. Therefore, the resources are vigorously assigned to a user according to his request, and relinquished after the job is done.

Cloud computing is a group of services as well as the hardware and operating system communications, the development of systems management software, system and platform, and virtualization components. According to the height of its resources, cloud computing services can be categorized into three categories, Infrastructure as a service (IaaS), Platform as a service (PaaS), and Software as a service (SaaS) [2].

As enjoying the ease of cloud computing, network security risks cannot be unnoticed. A customer's data security relies on protection service from cloud computing providers, however, current structure of cloud computing services are provided by self-regulating operators. At the First stage, the customer's information security gives business and management. At the Second stage, the information leakage can be caused by technology flows of providers. What's more, cloud computing is an open environment. Therefore, any flaws will cause information security risks of the whole system.

Cryptography in cloud computing (Crypto Cloud Computing) is a new protected cloud computing architecture. It can offer protection and safety of information security at the system level, and allows users access to shared services conveniently and accurately. Crypto cloud computing secures person's network with the outside world. It can secure the

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 4 Issue 1, Jan 2019
www.ijasrm.com
ISSN 2455-6378

individual protection without any delay of information exchange.

As Crypto cloud computing is based on the Quantum Direct Key system and QDK is a set of sophisticated asymmetric offline key mechanism. In this system, all elements get open and private key match as indicated by their ID. In this system, an entity can produce the public key of any other entities offline, no any third-party agency is necessary. Crypto cloud computing can avoid network traffic congestion, and other drawbacks of cloud data using current encryption system.

In the cryptographic cloud computing system, each object encrypts data using his/her own private key. All components in the framework, for example, cloud computing foundation units, stage, virtualization devices and every single included element have their own particular keys. While satisfying their own functions of information exchange and processing, all these elements will use the public key and private key to perform authentication first. Along these lines, crypto cloud framework guarantees the security and credibility of information exchange.

2 Review of Literature

A number of researchers have already been discussed the challenges of security that are raised by cloud computing. It is clearly mentioned that the security issue has played the most significant role in hindering the acceptance of Cloud Computing.
For security reason of cloud storage space, a variety of encryption techniques are being analyzed by researchers [3]. There are numerous security techniques which are presently applied to cloud storage. Apart from this there are still too many fields which require further enhancements like more efficient algorithms can be developed which can augment the security and protection level in the cloud storage.

The main focus here is the use and implementation of Cloud cryptography in order to efficiently protect the cloud data. The development in these areas has been increased as compared to previous years. With the use of advanced and enhanced algorithms and encryption techniques the cloud data will be securely stored and exchanged among the Corporate World.

3 Research Methodology

This research paper is based on the secondary data collected from the online sources, different research papers and from the Google Search Engine.

4 Security Issues

Cloud computing is a vast group of inter connected network. . There are different types of risk associated with the cloud network like data can be hacked by an unauthorized person. Data can be intercepted and changed by third party while transferring. The main issues in security of cloud data are related to data security include data integrity, data availability, data confidentiality, privacy, transparency of data and control over data where data resides [4]. There are different ways of achieving data security such as by providing various access controls and encryption methods. On the customer side, they ought to look into the security measures related to data that what are the security techniques are provided by cloud provider.

5 Existing Algorithms

1. DES (Data Encryption Standard)

DES (Data Encryption Standard) this algorithm is a symmetric block cipher developed by IBM. DES is an implementation of a Feistel Cipher. It utilizes 16 round Feistel structure. The block size is 64-bit. As the key length is 64-bit, DES has an efficient key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm [5]. The working of DES is depicted in the following illustration.

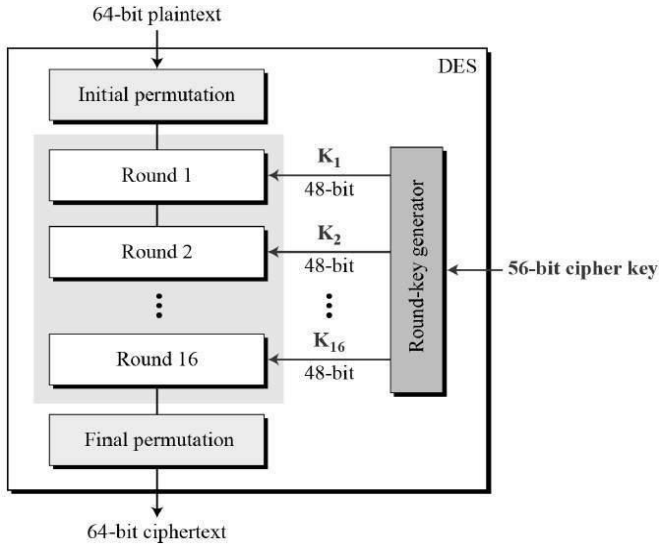

Fig:1Description of DES Algorithm

Triple DES (3DES)

The user primarily generate the 3TDES key K and then distributes it, which consists of three different DES keys K_1, K_2 and K_3, before using 3TDES, This means that Triple DES uses key of length

IJASRM
International Journal of Advanced Scientific Research and Management, Volume 4 Issue 1, Jan 2019
www.ijasrm.com
ISSN 2455-6378

3×56 = 168 bits. The encryption scheme is illustrated as follows:

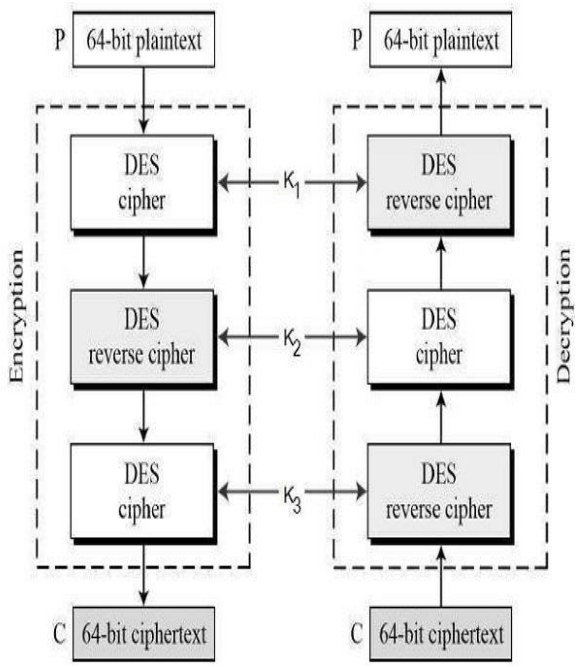

Fig:2 Encryption Procedure

The encryption-decryption process is as follows

- Encrypt the plaintext blocks of data using single DES with key K_1.
- Now decrypt the output of encrypted data in Step 1 using single DES with key K_2.
- At this step, encrypt the output of step 2 using single DES with key K_3.
- The output obtained after step 3 is the final cipher text.
- Decryption of a cipher text to plaintext is the opposite process. User first decodes or decrypts the data using K_3, then encrypt with K_2, and finally decrypt with K_1.

2. RSA Algorithm

The RSA (Rivest-Shamir-Adleman) algorithm is one of the most popular and secured public-key encryption algorithms [6]. This algorithm came into existence because it is very difficult to factor very large numbers. The working of this algorithm by using an encryption key (*e*,*n*), is define as follows:

1. Signify the message as an integer value between 0 and (*n*-1). Very large messages can be broken down into a number of blocks. Every block would then be corresponding by an integer in the same range.
2. Encrypt the plaintext message by raising it to the *e*th power modulo *n*. The result is a ciphertext message C.
3. To decode/decrypt the encoded message C, raise it to another power *d* modulo *n*

The encryption key (*e*,*n*) is made public. The key for decryption (*d*,*n*) is kept private by the user.

Calculate the Values for *e*, *d*, and *n*

1. Choose any two very large (100+ digit) prime numbers. Represent these numbers as *p* and *q*.
2. Set *n* equal to *p* * *q*.
3. Choose any large integer, *d*, such that GCD(*d*, ((*p*-1) * (*q*-1))) = 1
4. Find *e* such that *e* * *d* = 1 (**mod** ((*p*-1) * (*q*-1)))

Cryptographic methods cannot be proven secure. The RSA technique of achieving security based on the fact that it is extremely difficult to factor very large numbers. If numbers greater than 100 digit numbers are used for *p* and *q*, the resulting *n* will be approximately 200 digits. It is very difficult for the attacker to factor the numbers. Other methods for determining *d* without factoring *n* are equally as difficult. Any cryptographic algorithm which can prevent a rigorous attack is regarded as secure. At this level, the RSA algorithm is considered secure.

6 Comparison

Comparison of secret key and public key based DES and RSA algorithms is done. RSA removes the difficulty 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 vary from each other in certain features. Thus we find in decryption that DES is better than all other algorithms in throughput and power consumption. The main drawbacks of DES Algorithms are that it can suffer from key distribution and key agreement problems, But RSA consumes large amount of time to perform encryption and decryption operation. Simulation result showed that DES has better performance than RSA. It is assumed that throughput of DES algorithm is much better than the throughput of RSA algorithm. And 3DES has more power consumption and fewer throughputs than the DES due to its triple phase characteristics. It has been practically proved that decryption of DES algorithm is superior to other algorithms in throughput and less power consumption.

To overcome the limitations of DES and RSA algorithms and to make better use of both the algorithms, I make use of DES & RSA algorithm to produce encryption when user uploaded the plaintext files in Cloud Storage and converse DES & RSA algorithm to produce decryption when user download file from Cloud Storage, for increasing security. This projected system is considered to maintain security of text files only [6]. The process focuses on the following objectives which are accommodating in increasing the safety of data storage.

1) For Encryption of text files:

- Upload plaintext file to encrypt.
- Apply DES algorithm of Encryption to generate first level encryption.
- Apply RSA algorithm of Encryption to generate second level encryption.
- Store Cipher Text into Database.

2) For Decryption of text files:

- Read Cipher Text from Database.
- Apply RSA algorithm of Decryption to generate first level decryption.
- Apply DES algorithm of Decryption to generate Plain text.
- Display Plain Text to User.

7 Conclusion

Cryptography in cloud computing (Crypto Cloud Computing) is a new protected cloud computing architecture. It can offer security of information available at the system level, and allows users access to shared services conveniently and accurately. Crypto cloud computing secures person's network with the outside world. It can secure the individual protection without any delay of information exchange. In Our projected System, execution of the DES algorithm takes place to produce first level encryption. And then we apply the RSA algorithm on the encrypted output of DES algorithm to produce second level encryption. And identical procedure takes place for decryption using opposite DES and RSA algorithms. It means we applied multilevel Encryption and Decryption to provide security for cloud storage data. Cloud computing is distinct as the set of resources or services presented through the internet to the users on their demand by cloud providers. As each and every organization is transforming its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against several attacks.

References:

[1] Alexa Huth and James Cebula 'The Basics of Cloud Computing', United States Computer Emergency Readiness Team. (2011).
[2] Anitha Y, "Security Issues in cloud computing", "International Journal of Thesis Projects and Dissertations "(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.
[3] Qi. Zhang ·Lu. Cheng, Raouf Boutaba, "Cloud computing: state-Of-the-art and research Challenges", "The Brazilian Computer Society", April 2010.
[4] Garima Saini, Gurgaon Naveen Sharma,"Triple Security of Data in Cloud Computing ", Garima Saini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol.5 (4) , 2014
[5] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.
[6] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud ,"Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.