Multilevel Security in Cloud Computing

Rasmi M
Assistant Professor
Department of Computer Science and Applications
St.Mary's College, Thrissur-20

Abstract: **Cloud computing is the next big thing after internet in the field of information technology. It is an internet-based computing technology, in which software, shared resources and information, are provided to consumers and devices on-demand. Benefits of cloud storage are easy access, scalability, resilience, cost efficiency and high reliability of the data. Because of these benefits each and every organization is moving 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 unauthorized access, modification or denial of services etc. Privacy and security are the key issue for cloud storage. The proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud. In this paper, the proposed solution will be introduced to increase security in cloud computing. The multilevel encryption on cloud data is a method to secure data from access of unauthorized users. This method guarantees data protection.**

Keywords: Cloud computing, Cryptographic algorithm, AES, RSA, and Security.

1. INTRODUCTION

Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Cloud computing supports distributed service oriented architecture, multi-users and multi-domain administrative infrastructure, it is more prone to security threats and vulnerabilities. At present a major concern in cloud adoption is its security and privacy. Examples of cloud services include online file storage, social networking sites, webmail and online business applications.

Cloud computing is based on the principle of virtualization, which means that there is a single large machine and multiple clients are sharing this machine with a view that they have their own dedicated resources. It basically has three levels of services. First, Infrastructure as a service (IaaS), in this technique the hardware resources such as hard-disk, memory, networking resources etc are provided on rent and are charged as per the usage. Second, Platform as a service (PaaS), which not only provides all the facilities as in IaaS but also provides operating system facilities, their updates, etc hence make the overall work quite easy. Third, Software as a service (SaaS) which is the most flexible and easiest to use. It has all the features of IaaS and PaaS and moreover provides the freedom to choose software applications from a bundle of already available resources. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. NIST is the supporting community for cloud computing that gives the definition of cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Because of these benefits each and every organizations are moving their data to the cloud. Security and privacy issues are of more concern to cloud service providers who are actually hosting the services. In most cases, the provider must guarantee that their infrastructure is secure and clients' data and applications are safe by implementing security policies and mechanisms. While the cloud customer must ensure that provider has taken proper security measures to protect their information. The issues [2] are organized into several categories: trust, architecture, identity management, software isolation, data protection, availability, reliability, ownership, Data Backup, Data portability and conversion, Multiplatform Support and Intellectual property. To secure the cloud means secure the treatments (calculations) and storage (databases hosted by the cloud provider). Security goals of data include three points namely: Availability, Confidentiality, and Integrity. Confidentiality of data in the cloud is accomplished by cryptography. Cryptography is considered combination of three types of algorithms. They are (1) Symmetric-Key algorithms (2) Asymmetric-Key algorithms and (3) Hashing. Integrity of data is ensured by hashing algorithms.

Data cryptography mainly is the scrambling of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible, meaningless, during transmission or storage is termed Encryption. The main aim of cryptography is to take care of data secure from invaders. The opposite process of getting back the original data from encrypted data is Decryption, which restores the original data. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used. Cloud storage contains a large set of databases and for such a large database asymmetric-key algorithm's performance is slower when compared to symmetric –key algorithms.

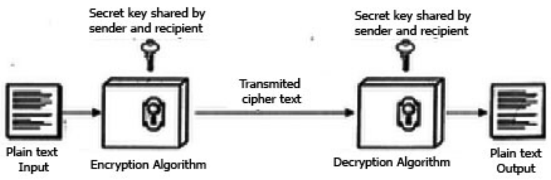


Fig.1. Simplified Model of Conventional Encryption

II. CLOUD DEPLOYMENT MODELS

There are three types cloud deployment models [3] that widely used are:

A. Public

It is referred as external cloud or multitenant cloud. This model represents an openly accessible cloud environment. Customer can access resources and pay for the operating resources. Public cloud can host individual services as well as collection of services.

B. Private

A private cloud provides a limited access to its resources and services to consumers that belong to the same organization that owns the cloud. It is also known as internal cloud or on premise cloud. In this, the infrastructure that is managed and operated for one organization only, so that a consistent level of control over security, privacy, and governance can be maintained.

C. Hybrid

A hybrid cloud is a combination of public and private cloud. It provides benefits of multiple deployment models. It enables the enterprise to manage steady-state workload in the private cloud, and if the workload increases asking the public cloud for intensive computing resources, then return if no longer needed.

D. Community

This deployment model share resources with many organizations in a community that share common concerns like governance, security, compliance etc. It typically refers to special-purpose cloud computing environments shared and managed by a number of related organizations participating in a common domain or vertical market [4].

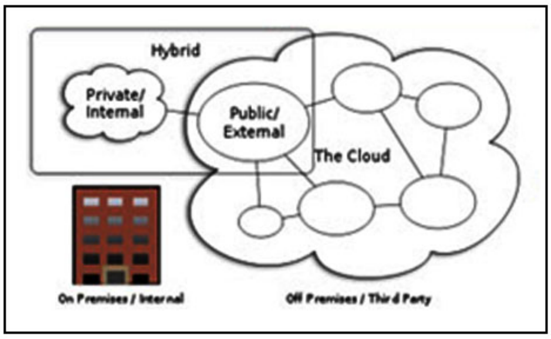


Fig.2. Cloud Deployment Models

III. EXISTING ALGORITMS FOR CLOUD SECURITY

In cloud storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, encryption algorithm [5] plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption where two keys-private and public keys are used. Public key is used for encryption and private key is used for decryption [6]. There are a number of existing techniques used to implement security in cloud storage. Some of the important existing encryption algorithms are as follows;

A. AES Algorithm

AES is the new encryption standard recommended by NIST to replace DES in 2001. AES algorithm can support any combination of data (128 bits) and key length of 128, 192, and 256 bits. The algorithm is referred to as AES-128, AES-192, or AES-256, depending on the key length. During encryption-decryption process, AES system goes through 10 rounds for I28-bit keys, 12 rounds for I92-bit keys, and 14 rounds for 256-bit keys in order to deliver final cipher-text or to retrieve the original plain-text. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For both encryption and decryption, the cipher begins with an AddRoundKey stage. However, before reaching the final round, this output goes though nine main rounds, during each of those rounds four transformations are performed; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns, 4) Add round Key.

In the final (10th) round, there is no Mix-column transformation. Decryption is the reverse process of encryption and using inverse functions: Inverse Substitute Bytes, Inverse Shift Rows and Inverse Mix Columns.

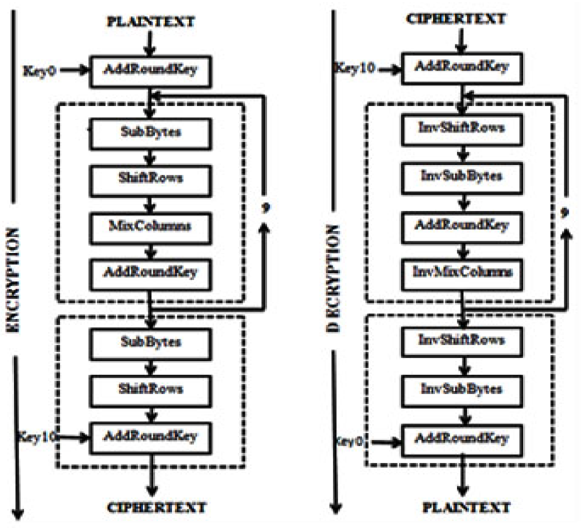
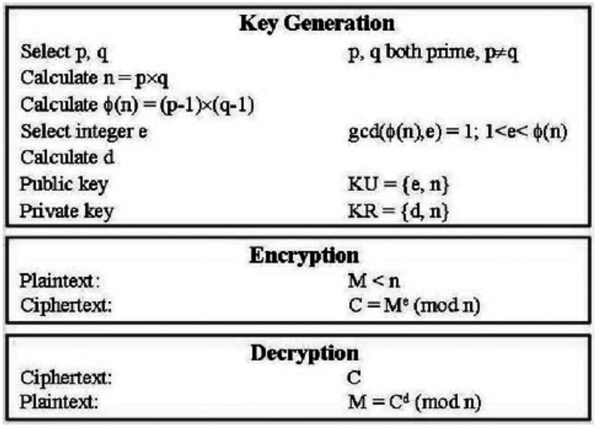


Fig.3. AES Algorithm

B. RSA Algorithm

This algorithm is known as RSA algorithm after the Ron Rivest, Adam Shamir and Len Adleman have designed it in 1977. It is an asymmetric key algorithm. RSA algorithm [7] is the method of encryption by using public key. The overall public keys are regularly known to everybody and are utilized for scrambling messages. The RSA algorithm architecture provides a mechanism that used to get secure communication as well as hiding the information from unauthorized users. RSA encryption algorithm helps to maintain confidentiality of data. This method is the first reliable method among other methods and it is one of the greatest advances in the field of cryptography. RSA utilizes measured exponential for encryption and decoding.RSA continues to be widely used in electronic transactions and it seems safe if it is used properly with long keys. RSA is generally composed of two keys, public key and a private key. Numerical key is fixed and it is used in computing the encryption. Public key to encrypt the message is clear to all. This message is opened only by the private key. In other words, anyone can encrypt a message but only the owner of the private key can open the message and read it. Suppose that the sender of the message has a pair of integers (e, n) as a public key to encrypt at his disposal. In contrast, the receptor of the message uses pair of (d, n) to decrypt the message. It is evident that two pairs of (e, n) and (d, n) have subtle relationship. This relationship is not in a way that we can simply deduce d by possessing e and n. All steps of the RSA algorithm are as follows:



Key Generation	
Select p, q	p, q both prime, p≠q
Calculate n = p×q	
Calculate $\phi(n) = (p-1)\times(q-1)$	
Select integer e	$\gcd(\phi(n),e) = 1;\ 1<e<\phi(n)$
Calculate d	
Public key	KU = {e, n}
Private key	KR = {d, n}

Encryption	
Plaintext:	M < n
Ciphertext:	$C = M^e \pmod{n}$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

Fig.4.RSA Algorithm

IV.PROPOSED SYSTEM

This system uses multilevel encryption and decryption [8] to provide more security for cloud storage. In personal cloud storage important data, files and records are entrusted to a third party, which enables data security. In cloud storage, any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources authentication of stored data becomes a mandatory task.

I have proposed a combination of two different security algorithms to eliminate the security challenges of Cloud Storage. I have taken a combination of two algorithms like AES and RSA. RSA is the first reliable method among other methods and it is one of the greatest advances in the field of cryptography. The AES algorithm can be used to strengthen RSA algorithm so that a high level security can be provided to the cloud data. The encryption and decryption of AES is very fast compared to other symmetric algorithms. RSA is an asymmetric key algorithm, the algorithm that uses different keys for encryption and decryption purposes. A user can upload the information in Personal Cloud Storage. When uploading the information, AES and RSA encoding schemes are used to encrypt data. The Block Diagram of proposed work at multilevel encryption is shown in following figure.

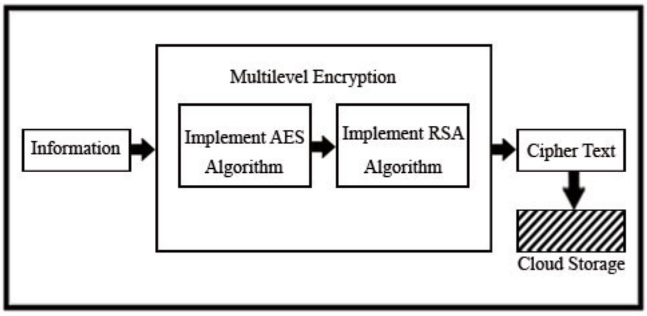


Fig.5. Multilevel Encryption

As Shown in figure 5, the steps of Multi-level encryption will be as follows;

- Upload the information
- Implement AES Algorithm to generate first level encryption
- Implement RSA algorithm to generate second level encryption
- Store the result into the database of cloud storage

And when downloading the file, apply RSA and AES algorithms for decrypting the data. The block Diagram of proposed work at multilevel decryption is shown in the following figure.

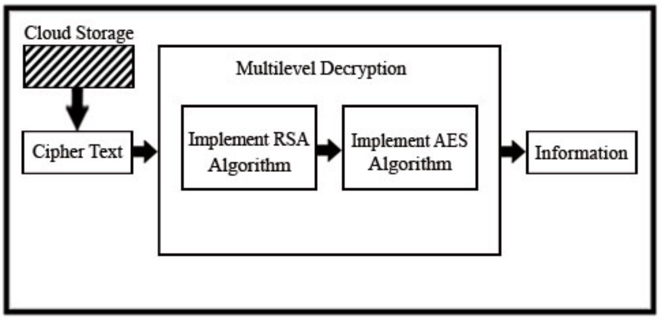


Fig.6. Multilevel Decryption

As Shown in figure 6, the steps of Multi-level decryption will be as follows;

- Take the encrypted data from the cloud storage
- Apply RSA algorithm to generate first level decryption.
- Use AES decryption algorithm on first level decryption data to generate Plain Text.
- Plain Text will be displayed to the User.

In the proposed System, I applied multilevel encryption and decryption to provide more security for cloud storage.

V. CONCLUSION

Cloud computing is defined as the set of resources or services offered through internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect the data against unauthorized access, modification or denial of services etc.

Cloud computing can become more secure using multilevel encryption and decryption algorithm. Because of this only the authorized user can access the data. If some intruder gets the data accidently or intentionally, he/she must have to decrypt the data at each level which is a very difficult task without a valid key. This multilevel security for cloud data will boost consumer confidence and attract more people to cloud platform. It is expected that multilevel encryption will provide more security for cloud storage than using single level encryption. My future work will explore this concept and a combination of algorithms will be applied either sequentially or parallel, to setup a more secure environment for data storage and retrieval.

REFERENCES

[1] Tyrone Grandson, E. Michael Maximilien, Sean S. E. Thorpe and Alfredo Alba. “Towards a Formal Definition of a Computing Cloud”. Published by IEEE 6th World Congress on Services 2010.

[2] Dr. L. Arockiam, S. Monikandan, “Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013.

[3] Mohit Marwaha, Rajeev Bedi, “Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing**”,** IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[4] Open Cloud Consortium.org.

[5] AL.Jeeva, Dr.V.Palanisamy and K.Kanagaram “Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms” International Journal Of Engineering Research And Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, pp.3033- 3037, May-Jun 2012.

[6] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, “Homomorphic Encryption Applied to the Cloud Computing Security”, World Congress on Engineering, Volume I, ISBN: 978-988-19251-3-8; ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online) , 2012.

[7] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences,Vol. 4, pp.141-146, March-May 2013.

[8] Shakeeba S. Khan, Prof.R.R. Tuteja, “Security in Cloud Computing using Cryptographic Algorithms”, International Journal of Innovative Research in Computer And Communication Engineering, Vol. 3, Issue 1, January 2015.