# Secure Storage and Replication using Hybrid Cryptographic Algorithm for Cloud Environment

**Sakshi Joshi**
Department of Information Technology
Institute of Engineering & Technology,
Devi Ahilya Vishwavidyalaya, Indore

**Arpit Agrawal(**Lecturer**)**
Department of Computer Engineering
Institute of Engineering & Technology,
Devi Ahilya Vishwavidyalaya, Indore

## ABSTRACT

**Cloud computing is the new generation technology provides the way of sharing of resources, memory, software anything in the form of service using internet. Subsequently, Cloud computing provides several advantages over the traditional network philosophy Involvement of public network make it sensitive for several security threat such replay attack, eavesdropping, man-in-middle attack. Basic function of any file system is to provide a long time reliable storage. Similar to a local based file system, Cloud file system stores files on one or more computers called servers, and makes them accessible to other computers called as clients, on the intranet in form of service.**

**Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (Saas). These are sometimes called the cloud computing stack, because they build on top of one another. Security is an important and unique phenomenon gives safe and isolated environment. Security model and principles are defined to implement security features with any applications. Confidentiality, authentication and integrity are primary principles for trust establishment. Existing work only concentrates on confidentiality concept during communication and does not imposes for integrity and privacy during storage.**

**A Secure storage can help to improve trust of user on cloud servers as well CSP and others. This work will implement security service architecture**
**Create safe and secure storage environment for cloud computing using web services and java technology.**

**Keywords:** ECC, AES, Storage, Replication, Cloud environment

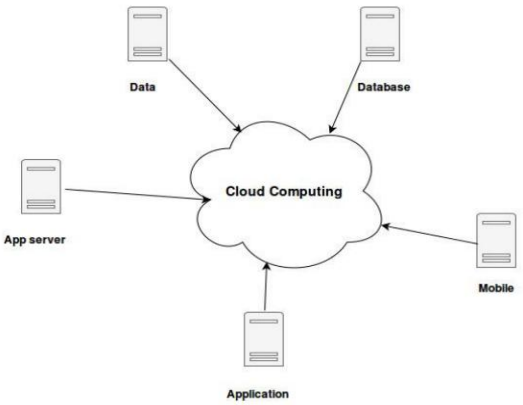
## 1. INTRODUCTION

Cloud computing is the one of the well-known field, which is one of the key resource in web-based applications. Cloud computing is the technology which includes Virtualization, parallel computing and distributed computing. Cloud computing is way to provide resources on demand; any resource can be use efficiently. Each cloud model consists of certain model, characteristics and deployment models. The cloud is not just technology which provides not just one service but package of so many services. Cloud computing is having one key component which is Internet; any service can be access with the help of browser. Service oriented architecture [2] is formed for having the cloud based services. The technology is not just confined to software but also to hardware, any hardware can be accessed. The benefit associated with cloud services is that high cost devices can be easily accessed.

Cloud computing is the process of providing services to user in according to their need. All the large enterprises are investing in very large amount in order to provide cloud services. Amazon, Google, Windows are having their own services which is available to all users in order to have efficient retrieval. In our survey it is find that homomorphic encryption is one of the finer encryption technique but the finest of all

encryption technique is elliptic curve encryption. In this work, the comparison of both computation is performed and result are depicted in order to prove the elliptic curve cryptography as better encryption technique.

Cloud computing realizes the importance of data sharing and thus creates the partition in order to have more feasibility. Cloud is partitioned as public , private and hybrid cloud. Organizations which wants the private access which means the storage within the surroundings are private cloud whereas if the storage and services are allowed in and out of the surrounding then it is called as public cloud. There are certain business areas where there is need of services in both




Figre 1. Cloud Computing

Environment which are in and out, hence for them hybrid cloud is used.

**1.2 Some Security Policies in Cloud:**

**1. Authentication**: Authentication is an important paradigm for cloud computing which can not changed ever, here authentication is important to confirm the identity of user and system through which user communicating. Third party service providers which are sometimes attackers, so the authentication of identity of the provider is important to check whether the service provider is attacker or trusted vendor. Authentication manages security risk.

**2. Confidentiality**: Confidentiality is equal to privacy. Some measures are taken to secure the information delivery to wrong person and making sure that right person will get the message. Authorized person has the right to access the data. If it falls under the hand of unauthorized person then the amount to damage cannot be imagined. Best example of confidentiality is data encryption in which authentication is a norm factor. For the transmission of sensitive information user id and password is important for authentication and encryption of that data creates confidentiality.

**3. Availability**: Maintenance of hardware is also important so to perform the correct functioning of operating system. Repair of hardware not functioning well will save time when the hardware is needed. Safety against data loss is important and interruption in connection can be lead to disaster event like fire. Which is the reason why maintenance of hardware is important?

**4. Integrity**: Integrity stands for accuracy, means data cannot be altered at the time of transmission by unauthorized person. Alteration of data is the activity done by unauthorized person when data transmits. They create error or delete some important data.

### 1.3 Service Models Of Cloud Computing:

Services of cloud are classified into three categories:

**1. PaaS (Platform as a service) :** Software as a service SaaS is essential and can be used easily from third party vendor. They provides applications which user as per there requirement use those applications and pay-as-per-use.

**2. Saas (Software as a service) :** PaaS Platform as a service creates the whole platform to the user so that he can work as he needed and has to pay for the use services. A platform to created to work on and the needed requirements are available to complete the work.

**3. IaaS (Infrastructure as a service) :** Infrastructure as a service, which provides virtual resources over an internet, it is managed and based over an internet. It reduces the cost of hardware and its implementation, also reduces time for managing hardware systems and their damages. The whole infrastructure is provided resources and customer can use what they require.

### 1.4 Types of Cloud:

On the basis of model cloud is classified in to four types:

**1. Public cloud:** Public cloud refers to the use of resources publically, anytime from anywhere, anyone can access the data & this data is provided free of cost from most of the service provider and many pay for it.

**2. Private cloud:** If any single organization owned the services then it is called private cloud. The owned resources are shared with organization only. External access is restricted. Private cloud is used due to security concern but private cloud is not preferred so much because of the high cost.

**3. Hybrid cloud:** Hybrid cloud is the combination of public and private cloud, it is combined so to get the best services which is possible. To get the best outcome public and private utilities are combined. We know that other cloud services are isolated; it can be private, public or community. To avoid many drawbacks of isolated cloud, hybrid cloud is used.

**4. Community cloud:** The organization owned it and maintains it for the particular community. Much organization can share it and managed internally and externally. Many organizations share its infrastructure for common reason.

### 1.5 Elliptic Curve Cryptography:

Elliptical curve cryptography (ECC) is based on public-key crypt-system in order to have fast accessing and retrieval of keys. Initially the encryption technique was based on the integer factorization problem but this cryptographic technique is based on elliptic curve equation. Previously large prime number are taken and there product are used as keys with the concept that it is tough to find the factor of product output. The level of security in ECC is so high that very small key size will help us achieving the security which other algorithm will achieve with very small size

## 2. LITERATURE REVIEW

### 2.1 Base Paper Work with diagram :

Babitha.M.P and K.R. Ramesh Babu," In cloud computing distributed resources are shared via network in open environment. Hence user can easily access their data from anywhere. At the same time there exist privacy and security issues due to many reasons. This paper addresses different data security and privacy protection issues in a cloud computing environment and proposes a method for providing different

security services like authentication, authorization and confidentiality along with monitoring in delay. 128 bit Advanced Encryption Standard (AES) is used for increase data security and confidentiality.

TABLE I. COMPARATIVE ANALYSIS BETWEEN AES, DES AND RSA

| Features | DES | AES | RSA |
|---|---|---|---|
| Developed | 1977 | 2000 | 1977 |
| Key Length | 56 bits | 128,192,256 bits | More than 1024 bits |
| Cipher Type | Symmetric block cipher | Symmetric block cipher | Asymmetric block cipher |
| Block size | 64 bits | 128 bits | Minimum 512 bits |
| Security | Not secure enough | Excellent secured | Least secure |
| Hardware & Software Implementation | Better in hardware than software | Better in both | Not efficient |
| Encryption and Decryption | Moderate | Faster | Slower |

Cloud and this data is stored temporarily. Afterwards the temporary data is stored permanently using RSA algorithm. Author stated that using RSA algorithm, security can be provided to data and data loss can be controlled. The implementation in RSA algorithm is done where public key, private key is used and secret key is also there which stores data permanently in cloud environment. RSA algorithm is very useful in terms of data security in cloud where data is uploaded and downloaded.

Uma Somani et al. In[3] author proposed about the authentication using digital signature which enhance the data security. Using this digital signature with RSA algorithm is very helpful in the medium of authentication of user. Through it, it can be detected that the user which is accessing data is authorized or not, his identity is valid or not. Authentication is the practice of detecting the attacker. Digital signature implies the identity of user in digital form which secures the data in cloud. A code which is generated and authenticated by encrypting it. Digital signature is an electronic transmitted document which identifies the identity of user.

Nicholas et al. In[4] introduces that virtualization is very important, software and hardware supports virtualization. Many hardware, operating system, infrastructure is virtualized and managed in cloud computing platform. After virtualization, dynamic and distribution is another characteristic of cloud. Dynamic is used for transforming physical resources. Distribution refers to the computation on physical node.

## 3. PROBLEM DOMAIN

With the rapid growth in cloud computing, Information Technology is also increasing. It is a large interconnected network which is widely used. Its services, platform etc are used by user. Services, platform and sharing are different thing, with all this, security is very important for storage and accessing of any data i.e. some mechanism are required which will provide security to the user and server of cloud. This feature of security is authentication, availability, confidentiality, and encryption. Authentication is an approach which ensures that request is from specific user and no interference will occur. If there is no trust relationship between sender and receiver then no third party provider is required.

If security is not provided to user then it is big risk to loss data and accessing of attackers. Many security mechanisms are applied in order to achieve trusted relationship between client and server.

Following problems were observed in proposed solution of existing paper:

1. There is low number of encryption solution for storage safety and replication.
2. Replication provides high data availability at the cost of inconsistency.
3. Maintaining consistency elevates the problem of increased data traffic but insecurity too.
4. An optimal solution to control the number of replicas and to consistently maintain these replicas with data traffic as reduced as possible with integrity maintenance.

5. AES perform slower than Rc6 and less secure than ECC.
6. Memory overhead of AES is also big issue.
7. Nowadays, all solutions are becoming data centric and need to provide safety during data storage.
8. Replication plays important role to improvise access time and performance.
9. Secure replication can help for easy and safe data storage and access.

## 4. Proposed System Solution

### 4.1 System Architecture:

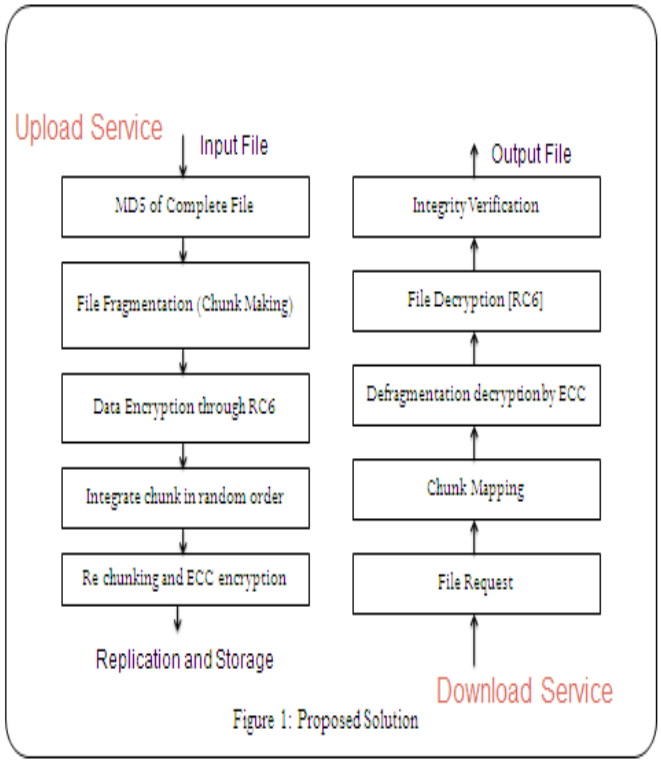



Figure 3: Proposed Solution

System architecture defines the complete work with the help of the above diagram, which explains as:

Following steps are suggested to provide safety during storage:

1. User will upload text file to be stored.
2. Initially, Message digest of whole file will be calculated to measure integrity factor of content at time of download.
3. RC6 algorithm will be used to encrypt the complete file to provide first level security.
4. Afterwards, Ciphered file will be divided into chunks to perform block cipher encryption.
5. Next, ECC algorithm will be used to encrypt each ciphered block to make two level encryption.
6. Replication and distribution technique will be used to replicate ciphered files and store on different location into multiple copies.
7. Vice versa, will be used for decryption purpose at time of download.

### 4.2 Objective:

1. To compute MD5 of overall file to maintain integrity
2. To develop a solution to encrypt file with RC6 algorithm.
3. To compute file size and divide file into chunks.
4. To develop a solution to individual chunk with ECC for strong secure storage
5. To implement solution for chunk management and replication.

### 4.3 System Configuration :

- 4 core Processor
- 4 GB RAM
- Internet Connection
- Ubuntu 14.04
- J.D.K 1.8

## 5. CONCLUSION

Despite of continues efforts to develop file replication and file consistency maintenance method in distributed system, there has been very little research devoted to tackling both challenges simultaneously. Proposed solution will not only help for replication management but also improve security during replication and chunk distribution.

## REFERENCES :

1. Babitha.M.P and K.R. Ramesh Babu," *Secure Cloud Storage Using AES Encryption*" published in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),International Institute of Information Technology (I²IT), Pune 2016**.**

2. Prof. Vishwanath S. Mahalle, "Implementing RSA encryption algorithm to enhance the data security of cloud in cloud computing", International journal of pure & applied research in engineering and technology, 2013, volume (8):220-227, ISSN-2319- 507X IJPRET.

3. Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC) – 28-30 Oct, 2010 IEEE.

4. (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longer important: the Internet great change of the high ground - cloud computing," The Big Switch:Rewining the World, from Edison to Google, CITIC Publishing House, October 2008.