Volume 3, Issue 5, May 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Enhanced Security Architecture for Cloud Data Security

**Dr. Chander Kant***
*DCSA, Kurukshetra University, India*

**Yogesh Sharma**
*DCSA, Kurukshetra University, India*

***Abstract— Cloud computing offers a prominent service for data storage known as cloud storage. The flow and storage of data on the cloud environment in plain text format may be main security threat. So, it is the responsibility of cloud service providers to ensure privacy and security of data on storage as well as network level. The following three parameters confidentiality, integrity and availability decide whether security and privacy of data stored on cloud environment is maintained or not. The proposed work is to define cloud architecture with configured samba storage and cryptographic encryption techniques. The cloud architecture deployed with samba storage uses operating system feature specifying permission values for three attributes (User/Owner, Group and Global) and maps it to cryptographic application which performs cryptographic operations. Cryptography application supports symmetric and asymmetric encryption algorithm to encrypt/decrypt data for uploading/downloading within cloud storage. A username and password based authentication mechanism for users and digital signature scheme for data authenticity are defined within cloud architecture.***

***Keywords— Cloud computing security, Cloud storage, Symmetric and asymmetric cryptosystem, AES, ECC, SHA, Samba Server, Cryptographic Application.***

## I. Introduction

Cloud computing is a distributed computing style which offer integration of web services and data centres. There are several major cloud computing providers including Amazon, Google, Yahoo, Microsoft and others that are providing cloud computing services. Amazon web services was first to provide an architecture for cloud based services in 2002 and after that advancements and new models for cloud architecture had been proposed and implemented. There have been many techniques of storing data on server storage. Such data storages provided by cloud service providers have to ensure client about Confidentiality, Integrity and Availability of data. Confidentiality: Confidentiality refers to keeping data private. Privacy is of importance as data leaves the borders of the owner**.** Confidentiality is supported by technical tools such as encryption and access control, as well as legal protection. Integrity: Integrity is a degree of confidence that what data is supposed to be in cloud, what is actually there, and is protected against accidental or intentional alteration without authorization. Availability: Availability means being able to use the system as anticipated by cloud user. Cloud technologies can increase availability through widespread internet-enabled access, but the client is dependent on the timely and robust provision of resources. Availability is supported by capacity building and good architecture by the provider, as well as well-defined contracts and terms of agreement. Cloud data storage security addresses the need of enforcing selective data access by providing an approach that supports the user in specification of access restrictions and security measures. Cloud Storage: Cloud storage [1] specifies the storage on cloud with almost inexpensive storage and backup option for small enterprise. The actual storage location may be on single storage environment or replicated to multiple server storage based on importance of data. Typical cloud storage system architecture includes a master control server and various clients. The mechanism model of cloud storage consists of four layers: storage layer which stores the data, basic management layer which ensures security and stability of cloud storage itself, application interface layer which provides application service platform, and access layer which provides the access platform. The basic cloud storage environment represented as follows:

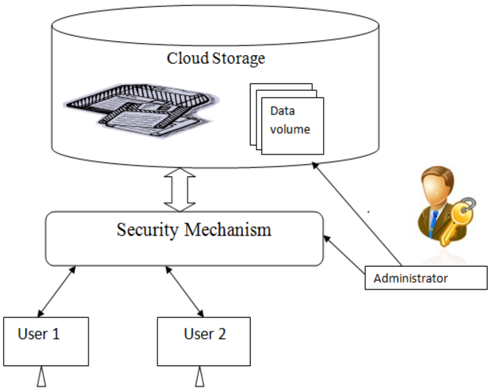


**Figure1. Cloud Storage Environment**

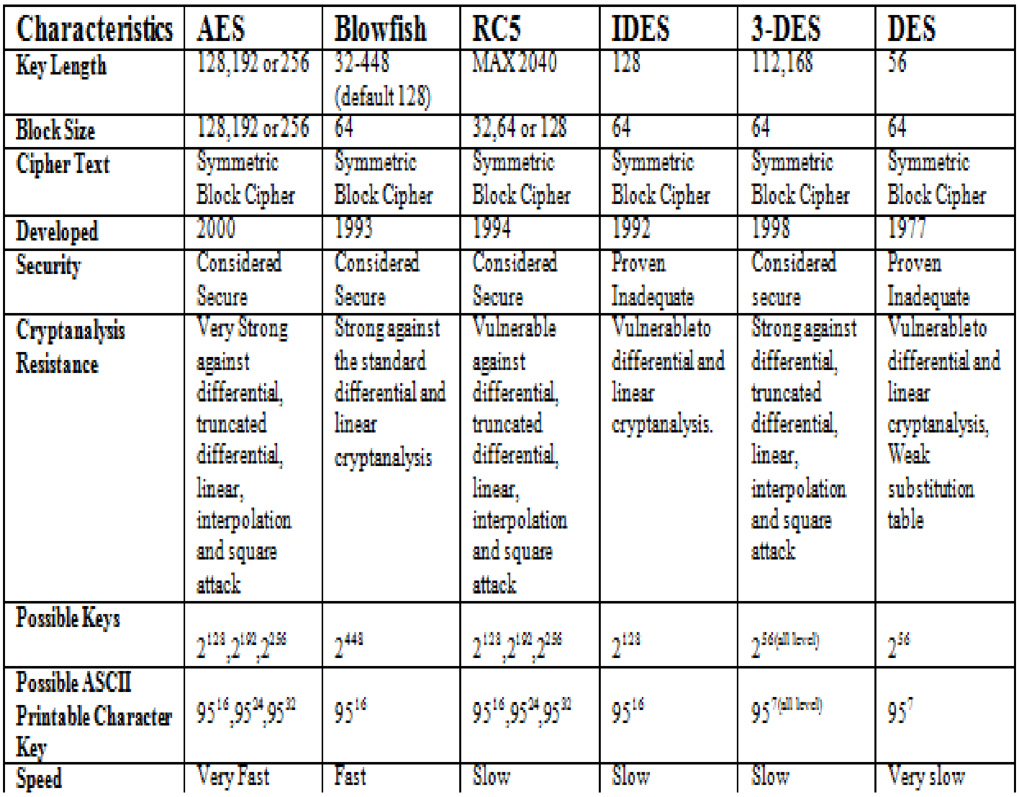
## II. Ensuring Data Security with Encryption Algorithm

The encryption algorithm is most commonly used technique to protect data within cloud environment. The data related to a client can be categorized as public data and private data. The public data is sharable among trusted clients that provide an open environment for collaboration. Private data is client's confidential data that must be transferred in encrypted form for security and privacy. According to key characteristics, modern cryptosystem can be classified [3] into symmetric cryptosystem and asymmetric cryptosystem. For a symmetric cryptosystem, the sender and receiver share an encryption key and decryption key. These two keys are the same or easy to deduce each other. The representatives of symmetric cryptosystem are DES (Data Encryption Standard), 3DES, RC5, RC6, Blowfish, Two-Fish and AES (Advanced Encryption Standard. For an asymmetric cryptosystem, the receiver possesses public key and private key. The public key can be published but the private key should be kept secret. The representatives of asymmetric cryptosystem are RSA (Rivest Shamir Adleman) and ECC (Elliptic Curve Cryptosystem).

## III. Related Work

The evaluation of various symmetric key encryption algorithms, asymmetric key encryption algorithms and Digital Signature algorithms are studied based on previous researches and different resources. The symmetric encryption algorithms studied are AES, DES, 3-DES, IDES, RC5, and Blowfish. There comparative study [6], [7], [8] based on attributes such as key length, block size, cipher text, developed, security, cryptanalysis resistance, possible keys, possible ASCII printable character key is described with the help of table:

Table1. Comparative study of various symmetric encryption algorithms



| Characteristics | AES | Blowfish | RC5 | IDES | 3-DES | DES |
|---|---|---|---|---|---|---|
| Key Length | 128,192 or 256 | 32-448 (default 128) | MAX 2040 | 128 | 112,168 | 56 |
| Block Size | 128,192 or 256 | 64 | 32,64 or 128 | 64 | 64 | 64 |
| Cipher Text | Symmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher | Symmetric Block Cipher |
| Developed | 2000 | 1993 | 1994 | 1992 | 1998 | 1977 |
| Security | Considered Secure | Considered Secure | Considered Secure | Proven Inadequate | Considered secure | Proven Inadequate |
| Cryptanalysis Resistance | Very Strong against differential, truncated differential, linear, interpolation and square attack | Strong against the standard differential and linear cryptanalysis | Vulnerable against differential, truncated differential, linear, interpolation and square attack | Vulnerable to differential and linear cryptanalysis. | Strong against differential, truncated differential, linear, interpolation and square attack | Vulnerable to differential and linear cryptanalysis, Weak substitution table |
| Possible Keys | $2^{128}, 2^{192}, 2^{256}$ | $2^{448}$ | $2^{128}, 2^{192}, 2^{256}$ | $2^{128}$ | $2^{56\text{(all level)}}$ | $2^{56}$ |
| Possible ASCII Printable Character Key | $95^{16}, 95^{24}, 95^{32}$ | $95^{16}$ | $95^{16}, 95^{24}, 95^{32}$ | $95^{16}$ | $95^{7\text{(all level)}}$ | $95^{7}$ |
| Speed | Very Fast | Fast | Slow | Slow | Slow | Very slow |

It was concluded from the above comparative study, that AES encryption algorithm is faster, more efficient, and superior in terms of time consumption (encryption/decryption) and throughput under the scenario of data transfer. So it would be better to use AES scheme in encryption of data stored at other end and need to decrypt multiple time.

The asymmetric encryption algorithms studied are RSA and Elliptic Curve Cryptography. These algorithms are compared [9] based on main attribute key size with various features such as key generation time, signature generation time and signature verification time are calculated and described in a table as follows:

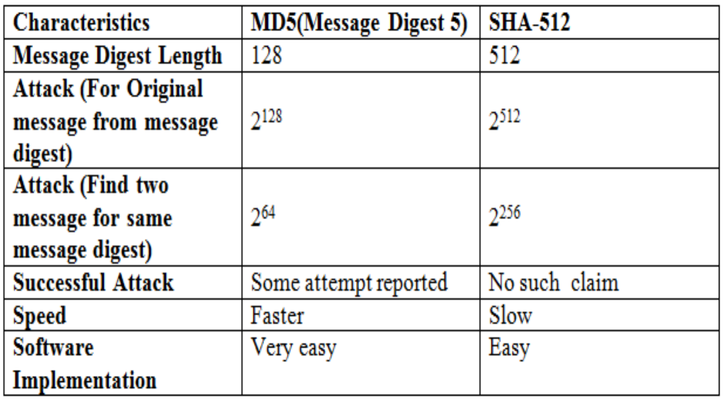
Table 2. Comparative study of asymmetric encryption algorithms

| Characteristics | Elliptic Curve Cryptography | RSA |
|---|---|---|
| Key Size (Bits) | 163 | 1024 |
| Key Generation Time (s) | 0.08 | 0.16 |
| Signature Generation (s) | 0.15 | 0.01 |
| Signature Verification (s) | 0.23 | 0.01 |

It was difficult to state which of asymmetric encryption algorithm is better because RSA performs better when there is no need to generate RSA keys for each use, but rather have fixed RSA keys. With RSA, signature generation and signature verification time is also much less than ECC. But ECC scores over RSA because of less key generation time. ECC is better option when lot of users connects to cloud based services with small session time like cloud based storage. That's why we have used ECC as asymmetric encryption algorithm for our cloud environment.

To achieve authentication and non-repudiation purpose within cloud computing environment digital signature has assumed great significance. There are various digital signature algorithms which involves the generation of message digest (hash). MD5 and SHA-1 are well known digital signature generation algorithms and comparative study of these are described with the help of table:

Table 3.Comparative study of digital signature algorithm



| Characteristics | MD5(Message Digest 5) | SHA-512 |
|---|---|---|
| Message Digest Length | 128 | 512 |
| Attack (For Original message from message digest) | $2^{128}$ | $2^{512}$ |
| Attack (Find two message for same message digest) | $2^{64}$ | $2^{256}$ |
| Successful Attack | Some attempt reported | No such claim |
| Speed | Faster | Slow |
| Software Implementation | Very easy | Easy |

The study shows that MD5 is much faster than SHA-512 digital signature algorithm, but with respect to security concerns SHA-512 is more secure than MD5 and no claim of successful attacks with optimal time complexity on SHA-512 has been done so far. The study of various cryptography (Symmetric/Asymmetric) encryption and digital signature algorithms helps to choose the best one from each category to be used in proposed cryptographic module. The symmetric and asymmetric encryption algorithms to be used are AES and ECC respectively. The SHA-512 digital signature generation algorithm is used in combination with ECC asymmetric key encryption algorithm. These algorithms are described as follows:

**AES (Advanced Encryption Standard):** The basic steps in algorithm [4] are stated as:

a) Key Expansion - round keys are derived from the cipher key using Rijndael's key schedule
b) Initial Round AddRoundKey - each byte of the state is combined with the roundkey using bitwise xor
c) Rounds-
    1. SubBytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
    2. ShiftRows - a transposition step where each row of the state is shifted cyclicallya certain number of steps.
    3. MixColumns - a mixing operation which operates on the columns of the state, combining the four bytes in each column.
    4. AddRoundKey
d) Final Round (no MixColumns)- 1. SubBytes 2. ShiftRows 3. AddRoundKey
e) Key generation- This module handles key generation by the cryptographic module at client side. The server generates unique keys for users once they authenticate themselves with the server. The key is generated using instances of AES key generator class. This key is then transferred to the cloud client via the mail-server through a mail which receives and stores a copy for it for decrypting purpose.

**Elliptic Curve Cryptography (ECC) with SHA-512:** An elliptic curve is given by an equation in the form of

$$y^2=x^2+ax+b \quad \text{where } 4a^3+27b^2\neq 0$$

The finite fields those are commonly used over primes ($F_P$) and binary field ($F_2^n$). The security of ECC is based on the elliptic curve discrete logarithm problem (ECDCP). This problem is defined as:

Given point X, Y on elliptic curve, find z such that X=zY. The following steps describe how ECC works with SHA-512 [9], [10].

ECC key generation**:** To generate a public and private key pair for use in ECC communication the steps followed are:

1. Find an elliptic curve E(K), where K is a finite field such as Fp or $F_2^n$, and a find point Q on E(K). n is the order of Q.
2. Select a pseudo random number x such that $1 \leq x \leq (n - 1)$.
3. Compute point P = xQ.
4. ECC key pair is (P, x), where P is public key, and x is private key.

Signature Generation: To create a signature S for message m, using ECC key pair (P, K) over E(k), the following steps followed:

1. Generate a random number k such that $1 \leq k \leq (n - 1)$.
2. Compute point $kQ = (x_1, y_1)$.
3. Compute $r = x_1 \pmod n$. If r = 0, go to step 1.
4. Compute $k^{-1} \pmod n$.
5. Compute SHA-512(m), and convert this to an integer e.
6. Compute $s = k^{-1}(e + xr) \pmod n$. If s = 0, go to step 1.
7. The signature for message m is S = (r, s).

Signature Verification: This part verify a signature s=(r,s) for message m over a curve E(k) using the public key P performing steps:

1. Verify r and s are integers over the interval [1, n - 1].
2. Compute SHA-512(m) and convert this to an integer e.
3. Compute $w = s^{-1} (\text{mod } n)$.
4. Compute $u_1 = ew \pmod n$ and $u_2 = rw \pmod n$.
5. Compute $X = u_1Q + u_2P$
6. If X = 0, reject S. Otherwise, compute $v = x_1 \pmod n$.
7. Accept if and only if v = r.

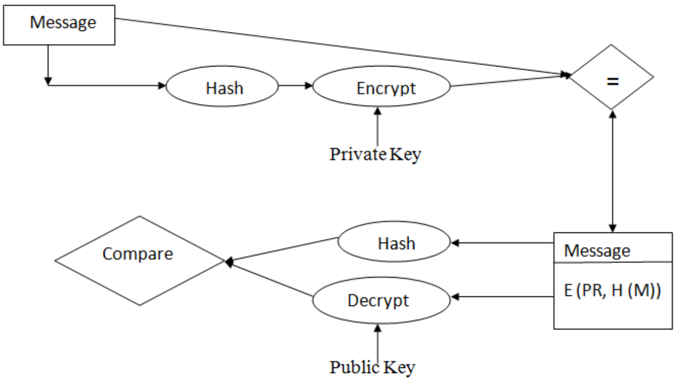


**Figure 2. Basic operation of Asymmetric Key encryption Algorithm with Digital Signature**

**Samba Server:** Samba server is used to provide file and print services to clients which are configured and provided with storage space on samba storage. Distributed file system environment that allow clients to access file and directories located on remote storage and treat those files and directories as if they were local. There is an inbuilt username and password based authentication mechanism for security. Samba supports all four DOS attributes but it map them to three attributes user, group and global with read, write and execute permission values. The group policies that samba supports are roaming profiles, folder redirections, login scripts and various system policies. Samba with data backup capability and storage partition can possibly supports workstation with cloud storage. The following are the basic steps to setup a samba storage environment:

a) Install samba package and edit samba configuration file /etc/samba/smb.conf.
b) Add clients to samba environment
c) Add share storage to smb.conf file.
d) Save and start Samba server
e) Access the share from any environment by connecting with samba server.

## IV. Proposed Work

The evaluation of various symmetric key encryption algorithms, asymmetric key encryption algorithms and Digital Signature algorithms are studied based on previous researches and different resources. The symmetric encryption algorithms studied are AES, DES, 3-DES, IDES, RC5, and Blowfish. There comparative study [6] [7] [8] based on attributes such as key length, block size, cipher text, developed, security, cryptanalysis resistance, possible keys, possible ASCII printable character key is described with the help of table:

Cloud architecture is designed by combining cryptographic algorithms with samba storage environment. The cryptographic algorithms to be used are selected based on comparative study from previous researches. So the symmetric, asymmetric and digital signature algorithms selected are AES, ECC and SHA respectively to be used for cryptographic application. The cryptographic application is used to encrypt and decrypt data, provides options to application user whether to use asymmetric with digital signature or symmetric algorithm. Samba server supports owner, group and global attributes associated with files/directories having possible values read, write and execute. Application users will decide whether to use AES algorithm, ECC with digital signature algorithm or disable encryption based on confidentiality, integrity and authentication level required on data which is to be stored on samba storage. The users are guided to select ECC with digital signature option for high level of confidentiality, authentication and integrity with data.

There must be some data that needs high availability among some users defined under a specific group. Another option with AES encryption algorithm supports user to encrypt data and define the group whose users can decrypt and use this data. The disable option provided with cryptographic application disable all options for user and supports upload/download functions without any cryptographic operation.

The security mechanism adopted for cloud architecture based on confidentiality, integrity and authenticity of stored data is a two level authentication mechanism.

1. Username and password based authentication mechanism: User is asked for a valid username and password provided at the time when samba clients are added with storage environment. The username and password are stored on samba storage verified and validated for every user logging storage area.
2. Key based authentication mechanism: This mechanism is supported with the help of mail server. While using cryptographic application for data encryption and decryption data secret key is generated for encryption using AES symmetric key encryption algorithm and same key is used for decryption of encrypted data. The data encrypted with symmetric algorithm is available for group users, so secret key is transferred to each group user through a mail server configured for each user. For data encrypted with asymmetric algorithm public key is transferred to user's mail server inbox for decryption process. The keys are stored within user's mail storage space.

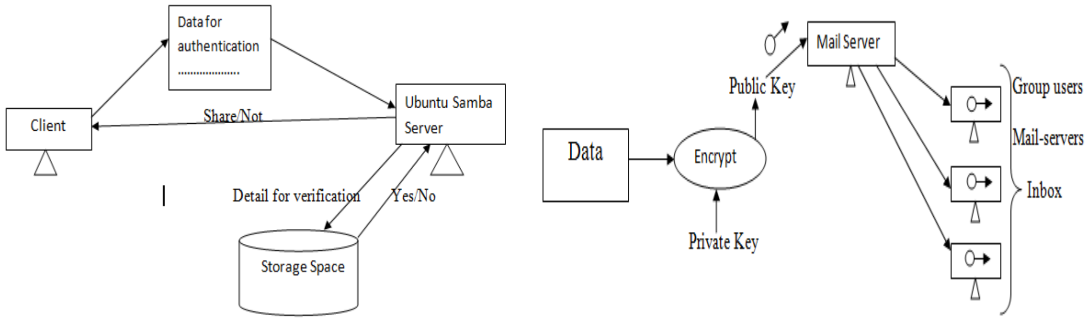


**Figure 3. Authentication based on username/password and key management using mail-server.**

**Proposed Cloud Architecture:**

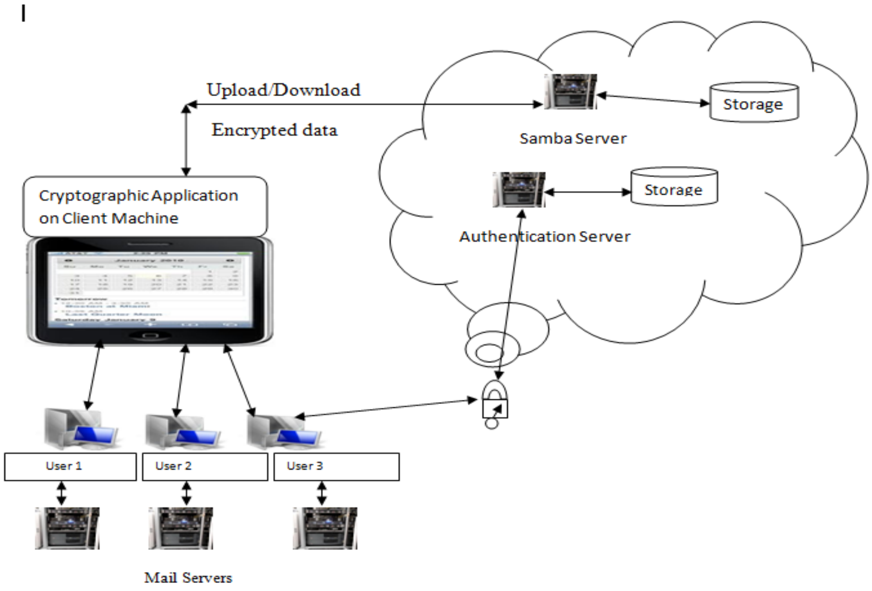


**Figure 4. Cloud Architecture with samba storage and advanced cryptographic application.**

Proposed Cloud architecture is enhanced security model for data storage within cloud environment. It consists of various users with local availability of mail server and cryptographic application. A cryptographic application installed on client side will connect user with samba storage and allows for encryption and decryption operation on data. As the cryptographic application is installed on client's machine it will increase speed-up ratio and mean processing [5] for encryption and decryption process. The authentication server used for authenticating users to enter into server environment and use available functionalities.

The various steps followed are explained in terms of communication among Client machine provided with cryptographic module and samba server storage.

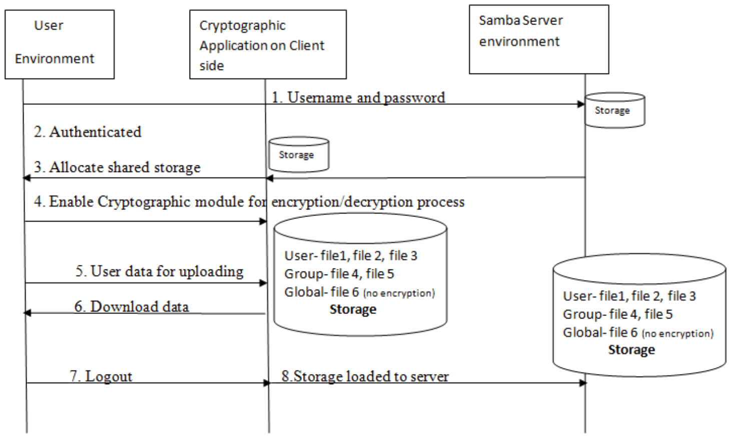

User Environment
Cryptographic Application on Client side
Samba Server environment
1. Username and password
Storage
2. Authenticated
Storage
3. Allocate shared storage
4. Enable Cryptographic module for encryption/decryption process
User- file1, file 2, file 3
Group- file 4, file 5
Global- file 6 (no encryption)
Storage
5. User data for uploading
6. Download data
User- file1, file 2, file 3
Group- file 4, file 5
Global- file 6 (no encryption)
Storage
7. Logout
8.Storage loaded to server

**Figure 5. Sequence diagram for describing interaction among samba server and user.**

Step 1: Username and password allocated to user for access to samba server storage.
Step 2: Verification and validation are performed by matching details stored in samba server storage.
Step 3: After user authentication storage is allocated to user for uploading and downloading.
Step 4: Cryptographic application based on AES and ECC with SHA used for encryption/decryption operation on data.
Step 5: The user provided with storage space decide to upload data using encryption application or directly on samba storage.
Step 6: Data downloaded from storage space and decrypted using key stored in user's mail server.
Step 7: After upload and download user logout from server storage.
Step 8: Storage loaded to server and connection terminated.

## V. Conclusion

The cloud architecture proposed in this paper brings convenient way to store and access files provided with confidentiality, integrity and authentication properties. Data is encrypted before uploading to server storage, so message confidentiality is preserved. On the receipt of encrypted message user can decrypt it using the key stored in mail server at the time of encryption enhancing authenticity. Decrypted message is used to generate Hash value verified with stored value ensures data integrity. The clients can privately store data or share data with group users in a secure way. The cloud architecture proposed is going to be cost-effective for institution lab setup and very small organizations. The possible enhancement in cloud architecture is to provide data backup and software migration with samba server and using some other cryptographic algorithm to implement cryptographic module.

## REFERENCES

[1] Arjun Kumar, Byung Gook Lee, HoonJae Lee, Anu, "Secure Storage and Access of Data in Cloud Computing", IEEE2012, P. 336-339.

[2] Bao Zhang, Changgen Peng, Zhipin Xu "Identity-based distributed cloud storage encryption scheme", IEEE 2011, pages 610-614.

[3] Mengmeng Wang, Guiliang Zhu, Xiaoqiang Zhang, "General Survey on Massive Data Encryption", P. 150-155.

[4] M.Sudha, M.Monica, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012, P. 32-37.

[5] Priyanka Arora, Arun Singh, Himanshu Tyagi, "Evaluation and Comparison of Security Issues on Cloud Computing Environment", World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 5, 2012, p. 179-183

[6] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms" Vol. 8, 2009, p. 58-64.

[7] S.Hirani, "Energy Consumption of Encryption Schemes in Wireless Devices Thesis," university of Pittsburgh, April 9, 2003.

[8] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, P. 84- 89.

[9] Nicholas Jansma, Brandon Arrendond, "Performance Comparison of Elliptic Curve and RSA Digital Signatures" April, 2004.

[10] Veerraju Gampala, Srilakshmi Inuganti, Satish Muppidi, "Data Security in Cloud Computing with Elliptic Curve Cryptography" vol. 2 Issue 3, July 2012.