Trust Enhancing Model for Cloud Environment

Kapil Kumar
M.Tech. Student
Computer Science Department
Geeta Institute of Management & Technology

Anurag Jain
Assistant Professor
Computer Science Department
Geeta Institute of Management & Technology

ABSTRACT
Cloud computing is a technology in which data can be stored and access at remote server without the installation of software as well as hardware being installed at client side. The quick growth in field of "cloud computing" has also increased data security concerns. Security is a constant issue for open systems and internet. When we are thinking about security, cloud really suffers a lot. Lack of security is the biggest hurdle in wide adoption of cloud computing. The weakness in user's authentication process, integrity and lack of effective security policy in cloud storage leads to many challenges in cloud computing. This paper proposes a scheme to securely store and access of data via internet. Authors have proposed a double encryption scheme that not only provides security of user's private data during storage and access over the cloud but also provides the authentication feature using Elliptic curve cryptography.

Keywords
Cloud Computing, AES, ECC, HmailServer, OTP.

1. INTRODUCTION
Cloud Computing is a technology that uses the internet and central remote servers to maintain data and applications. One of the most famous services offered by cloud computing is cloud storage. Cloud computing allows consumers and businesses to use applications without installation and access their individual files at any computer with internet access. This technology allows for much efficient computing by centralizing storage, memory, processing and bandwidth. Cloud computing is a model for enabling suitable, on-demand network access collection of customizable computing resources that can be rapidly provisioned and released with minimal management effort [14]. A data processing infrastructure in which the application software and often data reside on server`s side that is connected to the internet [12]

The major concern about cloud storage is security. With cloud storage server, users store their data on multiple third party servers. Users data saved on a remote storage system are at risk. There's always the possibility that a hacker will find and access data. Hackers could also try to take of the hardware on which data are stored. In another way, an annoyed employee could alter or destroy data using his or her genuine user name and password. Since all the data are in plaintext format, not only during the communication but also during storage on the servers, the data faces security threat.

In this paper, authors have proposed a security model which not only enhances the data confidentiality while it is stored at server end but also provides the authentication feature. The rest of this paper is organized as follows: Section 2 contains the building blocks of the proposed scheme. Section 3 gives the information about the proposed scheme. In section 4, authors have provided the security and efficiency analysis of the proposed scheme. Conclusion has been given in section 5.

2. BUILDING BLOCKS
During literature study authors have found the following algorithm as the useful tools for the implementation of security model proposed in section 3.

2.1 Advanced Encryption System (AES) [3, 4]
The AES **(**Advanced Encryption Standard) is the encryption algorithm given by NIST to replace DES. It is a symmetric-key block cipher algorithm. The AES algorithm has 3 fixed 128-bit block ciphers with cryptographic keys i.e. 128 bits, 192 bits and 256 bits. The size of key is unlimited, where the block size is maximum 256 bits. AES encryption technique is fastest, secured.

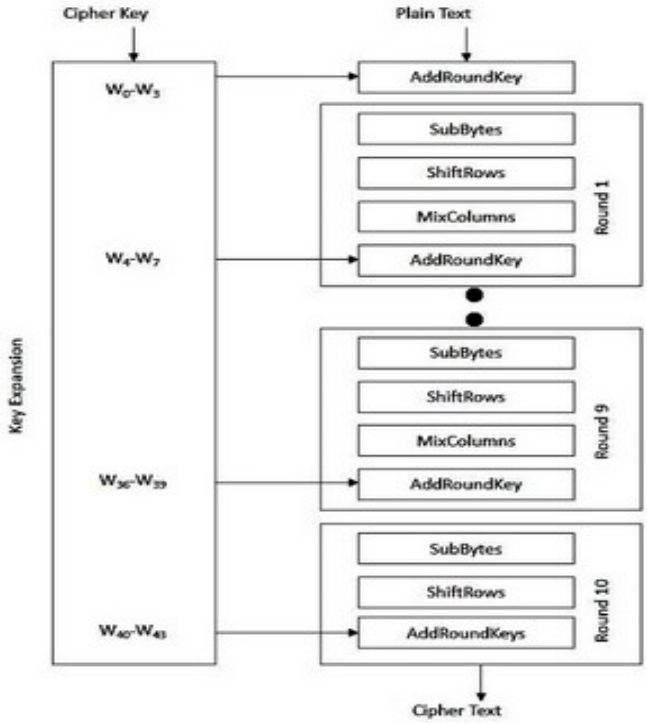

Figure 1: AES Encryptions Steps

AES is not vulnerable to any attack but Brute Force attack. However, Brute Force attack is not a simple job even for anyone. Because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which causes in millions of permutations and combinations. AES is also much faster than the conventional algorithms like RSA. It makes a fine choice for security of data on the cloud.16 byte encryption key, in the form of 4-byte words is expanded into a key schedule consisting of 44 4-byte words. The 4 x 4 matrix of bytes made from 128-bit input block represents a state array. Before any round-based processing for encryption can

begin, input state is XORed with the first four words of the schedule.

2.2 SHA-1[5, 6]

The acronym for SHA is Secure Hash Algorithm. The purpose of SHA1 is authentication not encryption. In SHA1, the user gives an arbitrary size of input and it produces a fixed size of hash function and the size of hash function for SHA1 is 160 bits. SHA-1 is a member of the Secure Hash Algorithm family unit. The four SHA algorithms are structured in a special way and are named SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 is the original version of the 160-bit hash function published in 1993 under the name SHA. It was not accepted by many applications.

2.3 Elliptic Curve Cryptography [7]

ECC is a public key cryptographic system based on the insolubility of certain mathematical problems. It was first recommended by Neal Koblitz and Victor S. Miller in 1985. An elliptic curve is given by the equation in the form of

$$y^2 = x^3 + ax + b$$

Where,

$$4a^3 + 27b2 \neq 0$$

Defined over an underlying field K, which can be a field over prime (Fp) or binary fields ($F2n$). Consider an elliptic curve in equation 1.

$$E: y^2 = x^3 + x + 1 \qquad (1)$$

If $p1$ and $p2$ are on E, where $p1 = (x1, y1)$, $p2 = (x2, y2)$, $p3 = (x3, y3)$ and $p1 \neq p2$ as shown in figure 2, then from the definition part we have

$$p3 = p1 + p2$$

Every user has the set of the public and private key, which are used for encryption and decryption respectively. It is an extension of the Diffe-Hellman key agreement scheme.

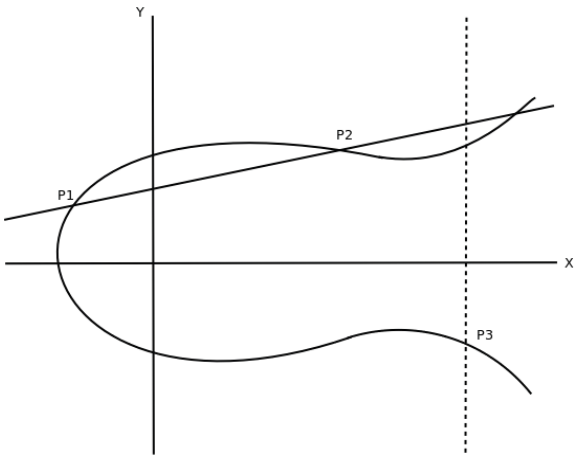

Figure 2: Elliptic curve

3. SECURITY MODEL

In the proposed model as shown in figure 3, double encryption, one at client side by the AES cryptography algorithm and second at the CSP server side by the ECC algorithm used. For authentication of user OTP (One Time Password) and username has been used for successfully login on CSP server. OTP will be generated automatically by CSP server. After successful login, server will send new refreshed OTP through HmailServer by CSP. The new refreshed OTP will be used at next time Login.

Whenever the user wants to upload confidential file on the server, user first encrypt that file by AES algorithm. AES algorithm converts the plain text file into cipher file c1. After the encryption, hash value will be generated by SHA-1 algorithm for future aspects regarding integrity of that file. After the successful AES encryption of the file by user, user will send that encrypted cipher on server and then the server algorithm starts working.

On the server side, ECC algorithm using public key encryption on the cipher c1 will generate cipher c2. SHA-1 algorithm at server side also generates the hash value regarding the cipher c2 file. The integrity of the file has been checked on both sides i.e. at server side as well as at user side. After the Public Key encryption of ECC, the CSP server sends the private key of ECC to User with the help of email by HmailServer. CSP Server will not maintain the logs of Private keys.

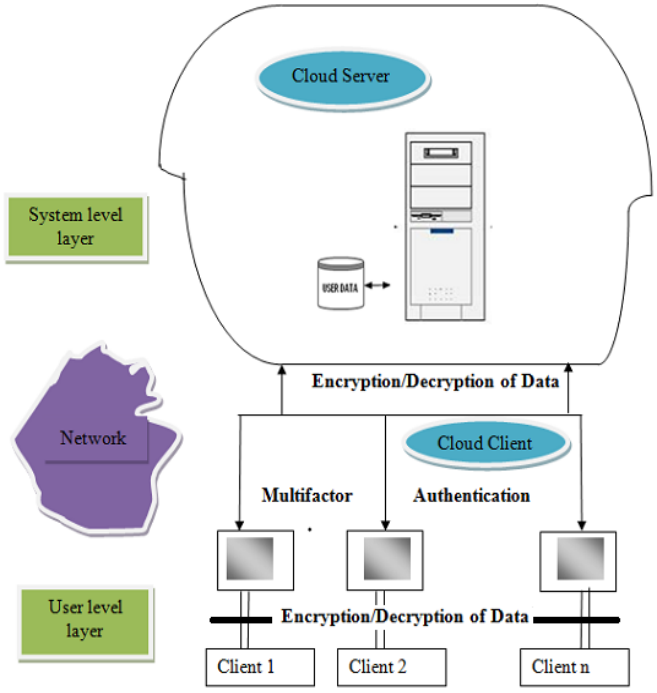

Figure 3: Proposed Model

The file is decrypted by the genuine user only, because to decrypt the file user needs the secret key of AES, Private Key of ECC algorithm. The user can download file from Cloud storage in encrypted form. During all the transmission the file is in encrypted form which results confidentiality. This method requires no additional software/hardware for authentication, nor there need to worry about the key management, because each time new key is generated for each file encryption operation which results in more security of the file.

Below are the different execution steps of proposed technique that enhance the security of data in Cloud by combining different mechanisms.

3.1 Assumptions

Users are already registered to the Cloud and if not, then first will have to register on CSP by filling registration form.

User must apply AES before uploading the file on CSP.

3.2 Login

- Secure authentication using username/password (OTP)
- Double authentication using refreshes OTP (user name+ Current Login Number) generation
- Encrypt (AES Secret Key || Operation || Method) on user side.
- Upload the encrypted file on Cloud Service Provider.
- Encrypt (ECC Public Key||encrypted File||Operation) on server side.
- Forward the Private Key to User Email.
- Downloading/ Uploading Data Encryption
- Data is retrieved and check Its Hash.
- Logout

In this paper, user first logins into the cloud and authenticates himself. After authentication user uses two techniques SHA-1 and AES key algorithm to encrypt and decrypt the data.

3.3 The Proposed Scheme

The Proposed Scheme involves the following steps:

3.3.1. Connection Establishment

The initial connection between user and CSP is established with the help of HTTP protocol before the creation of account in the system.

3.3.2. Account Creation

For the creation of account, user sends the request on the cloud service provider by filling the required form of user registration. Thereafter, the CSP send the OTP on the email Id of the valid user. The user does login on the CSP server by the OTP and the username. For the next time login by user, the HmailServer send the refreshed OTP to the user by email.

3.3.3. User Side Encryption

For sending the data on CSP server, user first encrypts the data by AES secret key encryption technique. After the encryption of data, its hash value is generated by SHA-1 algorithm. The SHA-1 generated the hash value of the cipher message or file for checking the integrity of the file in future by the user. The AES secret key is maintained by the user logs only.

3.3.4. Upload the Data on CSP server

After the AES encryption on the Client's file, AES creates its cipher text. The Change in proposed model is that the user uploads the cipher file of data on the server instead of plain file. In the proposed model CSP server unaware about the file contents due to sending the encrypted file to the CSP Server by the user. .It will increase the trustworthy of the user on CSP Server.

3.3.5. Server Side Encryption

After successfully uploading the file by the user, server again encrypt that cipher file with ECC public key encryption and send the private key of the ECC algorithm to user by email and remove the private key from the server database to maintain the security. The private key is send to user on its email id by HmailServer. After encrypt the file by CSP server, it also creates its hash value by the SHA-1 to check integrity on server side also.

3.3.6. User Side Decryption

For decryption of file, the user firstly downloads the file and then enters the ECC private key, AES secret key, which is used by the user at the time of encryption. The integrity of the file is also verified on user side and serves side by its Hash value

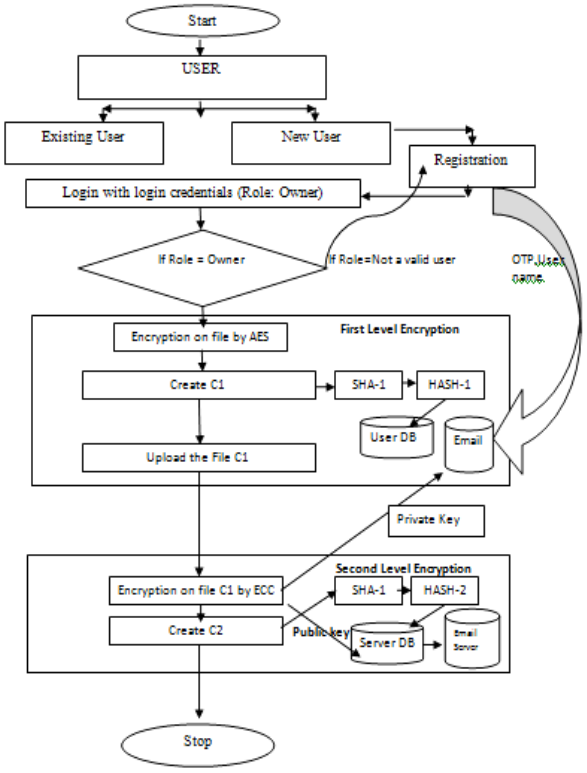

Figure 4: Encryption Algorithm

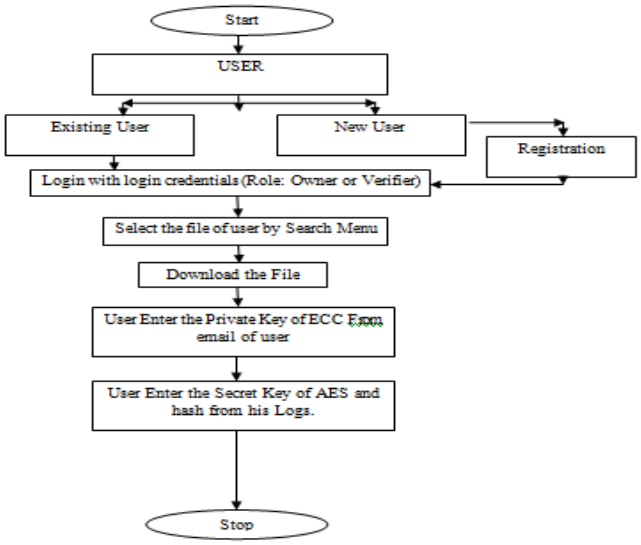

Figure 5: Decryption Algorithm

4. SECURITY AND EFFICIENCY ANALYSIS

4.1 Security Analysis [10, 11, 12]

The proposed model is highly secure communication model in which the concept of double encryption is used. As per study of many models, it has been found that the security level is

single side i.e. the security of file is either on user side in some models or on server side in some models whereas in the proposed model, authors have implemented the security enhancement by embedding the two different security algorithm on both side. It is very difficult for the opponent to check its plain text of the file after usage of both of the algorithms. Second thing is that the HmailServer which provide the security to the proposed model, as only the genuine user gets the email by HmailServer and thereby the ECC private key is send by the email server only to the genuine user. Strength of proposed model against different attacks has shown in table 1.

Table 1: Security analysis of model against diff. attacks

Sr. No.	Attack Name	How model defends?
1	Release of message contents	The proposed model user is not sending or uploading the plain text file. The release of message contents attack is prevented by the encryption technique at client's side as well as at server side
2.	Traffic analysis	Due to double encryption used in the purposed model, traffic analysis attack is prevented. AES secret key changes the key every time when it encrypts new file.
3.	Masquerade	The masquerade attack is prevented by the refreshed OTP send by the HmailServer. Each time the OTP changes whenever is used as password in purposed model.
4	Reply	The purposed model prevents this type of attack because of the email forwarded by the HmailServer.
5	Modification of messages	Unauthorized access is block by the refreshed OTP facility. As the file is being send by the user to CSP, the modification in file is prohibited, as it is already encrypted by Secret key.
6	Denial of service	Denial of service attack is prohibited by the Trusted CSP Server.

4.2 Enhancement on the Authentication

The authentication feature in our proposed model is highly secure. At the time of authentication, user OTP is directly known to the valid used and third person cannot login on the account of valid user. Proposed model made the authentication procedure more secure by use of HmailServer. The HmailServer provides the email method for the genuine users only whose email account exists. The data send to the CSP by user is encrypted form and to decrypt the massage the Key which is required only known to the user not the CSP server. At the time of login, if user is not entering a valid user name and OTP (which has been already sent to the user by HmailServer) then user cannot do login.

4.3 Enhancement on privacy preserving

The data send by the user on the CSP server is highly secure due to one encryption method from the user side and another encryption method on the server side. So, the CSP achieves the trust of the user. The user's trust and privacy preserving factor enhanced due to sending of the cipher file and not the plain text file. CSP also increases the privacy preserving of data by again encrypting the cipher file by doing ECC public key encryption and send the private key to the valid user only.

4.4 Improvement on integrity

The integrity of our purposed model is increased by double side integrity checking after the encryption of the file by user and the hash value is calculated in respect of the cipher file and is stored on the database of user. If any other person tries to change the file or even if changes the contents of the same, the user will come to know about such changes. Similarly on the server end, the hash value is generated by the SHA-1 algorithm and maintained by the CSP Server.

5. CONCLUSION AND FUTURE SCOPE

Data integrity, User's authentication, Security of data, privacy preserving and user trust are some of the most important security concerns in cloud computing. This paper aims to provide these security concerns over the private data which is stored at the public cloud. Authors have proposed a scheme to develop a trusted cloud storage system, which allows the users to store and access their data securely in the cloud by encrypting the data in the client side and server side. Since the private key of ECC and AES secret key is owned by the user of the data, no one else can decrypt the data. HmailServer Send the ECC private key to the valid user only.

In future, author's emphasize is on the implementation of proposed system to test on real applications and the creation of user's account on HmailServer automatically at the time of user registration

6. REFERENCES

[1] Mell, P. and Grance, T. (2009), "The NIST Definition of Cloud computing", National Institute of Standards and Technology, vol. 53, no. 6.

[2] Ghobadi, A., Karimi, R., Heidari, F. and Samadi, M. (2014), "Cloud computing, reliability and security issue," 16th International Conference on Advanced Communication Technology (ICACT), pp. 504-511.

[3] Surv, N., Wanve, B., Kamble, R., Patil, S. and Katti, J. (2015), "Framework for client side AES encryption technique in cloud computing", 2015 IEEE International Conference on Advance Computing Conference (IACC), pp. 525-528.

[4] Rewagad, P. and Pawar, Y. (2013), "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", International Conference on Communication Systems and Network Technologies (CSNT), pp. 437-439.

[5] Kaur, R. and Singh, R. P. (2014), "Enhanced cloud computing security and integrity verification via novel encryption techniques", International Conference on Advances in Computing Communications and Informatics (ICACCI), pp. 1227-1233.

[6] Shimbre, N. and Deshpande, P. (2015), "Enhancing Distributed Data Storage Security for Cloud Computing Using TPA and AES Algorithm", International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 35-39.

[7] Yin, X. C., Liu, Z. G. and Lee, H. J. (2014), "An efficient and secured data storage scheme in cloud computing using ECC-based PKI", International Conference on Advanced Communication Technology (ICACT), pp. 523-527.

[8] Chakraborty, T. K., Dhami, A., Bansal, P. and Singh, T. (2013), "Enhanced public auditability & secure data storage in cloud computing", IEEE 3rd International Conference on Advance Computing Conference (IACC), pp. 101-105.

[9] Singh, S. and Kumar, V. (2015), "Secured user's authentication and private data storage- access scheme in cloud computing using Elliptic curve cryptography", 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 791-795.

[10] Prodanovi, R., and Simi, D. (2007)," A Survey of Wireless Security", Journal of Computing and Information Technology – CIT, pp. 237–255.

[11] Kumar, U., and Gambhir, S. (2014), "A Literature Review of Security Threats to Wireless Networks", International Journal of Future Generation Communication and Networking, Vol. 7, No. 4, pp. 25-30

[12] Djenouri, D., Khelladi, L. and Badache, A. N., "A survey of security issues in mobile ad hoc and sensor networks", Communications Surveys & Tutorials, IEEE, vol. 7, no. 4, pp. 2-28.