PRESERVING PRIVACY BY INTEGRITY AUDITING FOR SHARED CLOUD DATA

S.Radhika[1], M.Sukumar[2]

[1] *PG Scholar, Department of Computer Science and Engineering, Sri Vidya College of Engineering & Technology, Virudhunagar.*

[2] *Assistant professor, Department of Information Technology, Sri Vidya College of Engineering & Technology, Virudhunagar.*

ABSTRACT

Cloud computing is a popular technology that delivers computing services over the Internet. By using these services data can be stored and access/retrieve at remote servers without installing any software. The rapid growth of cloud computing has also increased the security concerns of user data. For open systems and Internet the security is considered as a major issue. While intending about security, the cloud extremely suffers a lot and the lack of security is a major obstruction in wide user selection of cloud computing. In this paper, we are going to propose a novel technique to store and access/retrieve data through Internet. Here a double encryption technique is proposed which can provide security of user's private data on storage and access/retrieve throughout the clou d. It uses Elliptic curve cryptography in order to provide the authentication feature.

Key Words: *Cloud computing, Advanced Encryption Standard, Elliptic curve cryptography and SHA-1.*

1. Introduction

Cloud computing is a famous technology which employs the Internet and central control of remote servers to keep up information and applications. A standout amongst the most popular services provided by cloud computing is distributed/cloud storage. Cloud computing permits users and organizations to utilize ap plications without any installation and access their individual documents at any computer by using access. [1]. This technology takes into consideration of much efficient computing with centralized storage, bandwidth and memory. Cloud computing is an example for empowering desirable, on-demand network access by the accumulation of adjustable computing resources which can be quickly provisioned and discharged with negligible administration exertion. A data processing infrastructure where the application software and user data are often reside on server`s side which is connected to the internet [2,3].

The significant concern about distributed storage is security. With distributed storage server, users/clients store their information on numerous third party servers. Storing user's data on remote storage server are at high risk. Always there is a probability that a hacker can discover and access user's data and the hackers can also attempt to get the hardware on that user's data stored. [4]. In another way, an irritated worker could adjust or decimate information utilizing his or her bona fide user name and password word. Because all the information is in the format of plaintext not only during the data transmission but also during data storage on the centralized servers in which the stored data faces security threat. [5].

In this paper, a novel technique is proposed which not only increases the data confidentiality when it is stored at centralized server but also offers the authentication feature. The rest of the paper organizes as follows.

2. Related work

A large amount of researchers have committed significant concentration to the troubles on how to securely outsource local pile up to remote cloud server. The problem of remote data integrity and availability auditing attacks the attestation of many researchers. *Sagarika Dev Roy, et.al (2014)* proposed a methodology for secure outsourcing of linear Computations into the cloud environment. Outsourcing is a common procedure engaged in the business world when the customer chooses to farm out a certain task to an agent for the benefit of the firm in terms of time and cost. They proposed methodology to detecting a malicious server, in an efficient result verification method.

YongjunRen, et.al (2012) proposed designated verifier provable data possession. This plays a major role in public clouds. Designated verifier provable data possession is a matter of crucial importance when the client cannot perform the remote data possession checking. By using the system security model and homomorphism authenticator they designed a new scheme. The scheme removed luxurious bilinear computing process. Furthermore in this proposal, the cloud storage server is stateless and independent of the verifier. This is an important secure property of any other schemes. In the course of security analysis and performance analysis, their scheme is secure and high efficiency.

FrancescSebe, et.al (2008) proposed a methodology to check the efficent of remote data control or possession. For checking the data possession in a complex information system such as power facilities, airports, data vaults, and defence systems is a matter of vital importance. Data possession checking protocols permits us to check a remote server is able to admission an uncorrupted file. In such a way that the verifier need not to know about the whole file, that is going to be verified. Regrettably, present protocols only allow a limited number of successive verifications or just the impractical from the computational point of view. In this presents a new protocol for remote data possession checking.

Giuseppe Ateniese, et.al (2008) proposed a methodology to operate on the remote storage data in a high secured manner. The main concern is how much frequently, efficiently and securely the system will verify that a storage server is realistically storing its client's. Key thing is the clients' outsourced data are potentially very large. The storage server is assumed to be not trusted in terms of both the security and reliability. It might unkindly or unintentionally wipe out data being hosted. But the problem is exacerbated by the client being a small computing device with partial resources. Previous work has deal with this problem that is use public key cryptography or outsource its data in encrypted structure. In this paper, they constructed a extremely efficient and secure technique based completely on symmetric key cryptography. If detection of any modification or deletion of small parts of the file is important then erasure codes could be used.

Jiawei Yuan, et.al (2014) proposed a new method based on some modern procedures such as based on authentication polynomial tags and linear authenticators. Data integrity auditing is achieved concurrently in this approach. The proposed idea is to characterize the constant real time communication and also the computational cost on the users' side. It supports both public auditing along with batch auditing process. The security of our proposed scheme is fully based on the Computational Diffie-Hellman hitch. Many data loss and corruption events are reported against the well known cloud service providers, data owners, to resolve these issues they need to periodically audit the integrity of their outsourced data. And also every cloud service providers must improve their efficiency of cloud storage. To minimize the unnecessary redundant copies, the cloud storage servers would be duplicating the data. By having only one or few copies for each file and making a link to the file for every user who asks the same file stored in the disk.

3. Techniques Used

3.1. AES

NIST has given the AES (Advanced Encryption Standard) algorithm in order to replace DES algorithm. The AES is an encryption algorithm which is otherwise known as symmetric-key block cipher algorithm. The AES algorithm contains three fixed 128-bit block ciphers with cryptographic keys i.e. 128, 192 and 256 bits. The key size is unlimited and the block size is up to 256 bits. AES encryption algorithm is faster and secured. [6].

Except Brute Force attack, the AES is not vulnerable. Nevertheless, the Brute Force attack is not an elementary task even for anyone. [7]. Since, the size of encryption is utilized by the AES algorithm is of the order 128 bits, 192 bits and 256 bits that induces in millions of permutations and combinations. Computation of AES algorithm is much faster than the traditional RSA algorithm. It causes a fine choice for data security on the cloud. A state array of 4×4 matrix is made from the 128-bit input block.

3.2. Elliptic Curve Cryptography

ECC is a type of public key cryptographic system which is based on the unsolvability of certain mathematical problems which is encouraged by Neal Koblitz and Victor S. Miller in 1985. [8]. The following equation represents an elliptic curve which is given by,

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

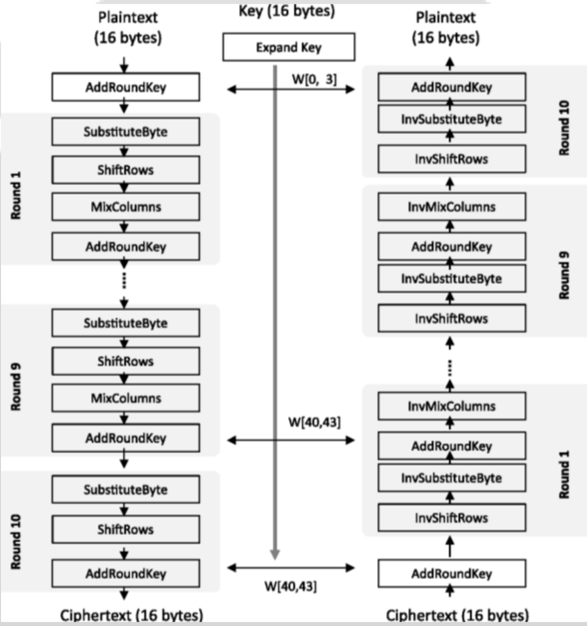

Figure 1: AES Algorithm

Where

$$4x^3 + 27y^2 \neq 0$$

Characterized over a basic field k , that can be a field over prime F_P or binary F_b fields. Let us take an elliptic curve in equation 1.

$$E : b^2 = a^3 + a + 1$$

If q_1 and q_2 are on E , where $q_1 = (a_1 b_1)$, $q_2 = (a_2, b_2)$, $q_3 = (a_3, b_3)$ and $q_1 \neq q_2$, then from the part of definition we have

$$q_3 = q_1 + q_2$$

Every user in the network has a set of public and private keys that are employed for data encryption and decryption respectively.

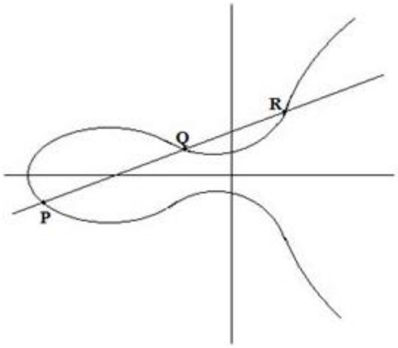

Figure 2: ECC Algorithm

4. Proposed Technique

In our proposed technique double encryption is used in which one is used at the client side by using AES encryption algorithm and another one is used at the CSP server side by using ECC algorithm. Here OTP (One Time Password) and username has been employed for authentication of user to login on the CSP server. The CSP server automatically generates the OTP and the CSP server will send a new OTP via Hmail Server after the successful login process. This new OTP is employed for next login. When the user needs to upload confidential data on the CSP server, he/she must encrypt that data by using AES algorithm. The AES algorithm is applied by converting the plain text to the cipher text. Then the user sends the encrypted cipher c1 data on the CSP server after that the server algorithm will start working. On the other hand the ECC algorithm generates cipher c2 by using public key encryption on the cipher c1 at the server side.

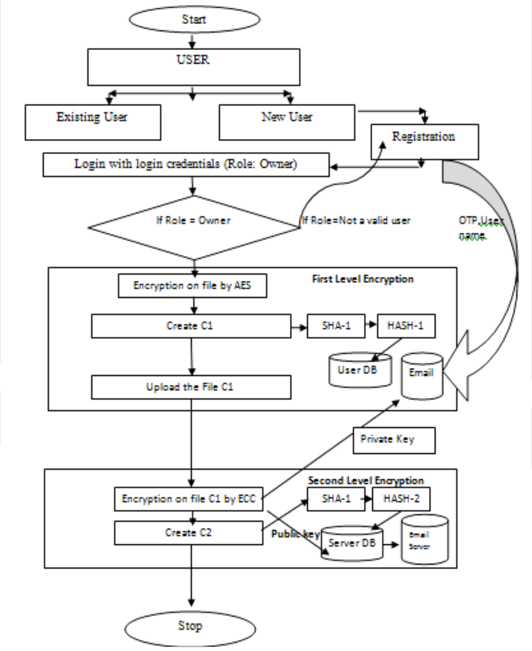

Figure 3: Encryption Algorithm

On server and user side, the data integrity has been checked. The CSP server will send the private key of ECC to the user after completion of Public Key encryption of ECC algorithm through email by the Hmail Server. Note that the CSP will not keep up the Private Key logs.

The user document is decrypt by an authentic user only since secret key of AES and Private Key of ECC algorithm are used to decrypt user document. In cloud storage the user document present in the encrypted form that results confidentiality. This technique needs no extra software/hardware for data authentication. Thus there is no need to about the key management. Since each and every time a new key is generated for every document encryption process that results in much more security of the document. Our proposed technique involves the following steps.

4.1. Connection Establishment

The HTTP protocol is used to setup the initial connection between user and CSP server before create an account in the system.

4.2. Account Creation

In order to create an account user must send a request to the cloud service provider by filling the required form of user registration. After that the CSP server will send the OTP to the email ID of legitimate user. Then the user can login to the CSP server by using the OTP and the username. The HmailServer will send the new OTP to the user's email ID for next time login.

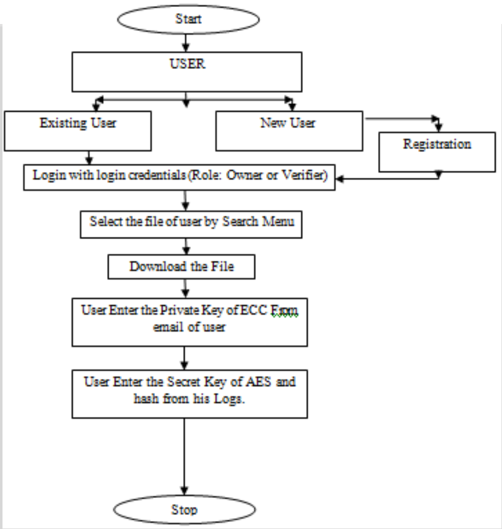
Start
USER
Existing User
New User
Registration
Login with login credentials (Role: Owner or Verifier)
Select the file of user by Search Menu
Download the File
User Enter the Private Key of ECC From email of user
User Enter the Secret Key of AES and hash from his Logs.
Stop

Figure 4: Decryption Algorithm

4.3. User Side Encryption

At first the user must encrypt the data by using AES secret key encryption technique to send the data on the CSP server. SHA-1 algorithm is used at the user side to generate hash value of the encrypted data and it also generates the hash value of the document in order to check the integrity of the document in future. The user logs keep up the AES secrete key.

4.4. Upload the Data on CSP server

After completion of the AES encryption on the user's document, the AES generates its cipher text. In our proposed model the user uploads the cipher text instead of plain text of the document. Here the CSP server insensible of the file contents because of sending the encrypted document to the CSP server by the user. Therefore it will increase the confidentiality of the user on CSP Server.

4.5. Server Side Encryption

When the CSP server receives any user's cipher document it again encrypt by using ECC public key encryption. Then it sends the private key of the ECC algorithm to the corresponding user through email and then it removes the private key from the CSP server database in order to maintain the security. Through HmailServer the private key is send to the users to their email ID.

5. Performance evaluation

Our proposed technique provides highly secure communication by applying the concept of double encryption. According to several study of numerous techniques the security level is single side that is the security of document is either on the user side with few techniques or on the server side with few models though in the proposed technique. But here we have executed the security improvements by appling the two diverse security algorithms on both side. It is extremely difficult for the rival to check its plain text of the document after utilization of both algorithms. Next the HmailServer provides the security to the proposed technique so literal user can only receives email through HmailServer. Therefore the literal user can only obtain the ECC private key through the email server.

6. Conclusion

In cloud computing, authentication, user trust and authentication, data integrity and privacy preserving are considered as the most significant security criteria. In this paper we discuss about the security issues over the private data that is stored public cloud. Here a novel technique is proposed to formulate a confidential cloud storage system that permits the users to store and retrieve/access data on the cloud securely by encrypting the data on the user and server side as well. Subsequently the user data contains the secrete key of AES and private key of ECC which cannot decrypt by anyone. The legitimate user only can receive the private key of ECC through the HmailServer.

7. 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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.