DOI: https://doi.org/10.24113/ojsscience.v3i10.148

Design and Implementation of Hybrid EC-RSA Security Algorithm Based on TPA for Cloud Storage

Arshi Jabbar
M.Tech Scholar
Department of CSE
NRI
Bhopal, M.P., India
arshi.jabbar@gmail.com

Dr. Umesh Lilhore
HOD
Department of CSE
NRI
Bhopal, M.P., India
umeshlilhore@gmail.com

***Abstract* - Cloud storage is one among the service provided by Cloud computing within which information is maintained, managed, secured remotely and created available to users over a network. The user concerning about the integrity of data hold on within the cloud because the user's data will be attacked or changed by outside attacker. Therefore, a new thought referred to as information auditing is introduced that check the integrity of knowledge with the assistance of an entity referred to as Third Party Auditor (TPA). The aim of this work is to develop an auditing scheme that is secure, economical to use and possess the capabilities like privacy conserving, public auditing, maintaining the information integrity together with confidentiality. It comprises 3 entities: data owner, TPA and cloud server. The data owner performs numerous operations like splitting the file to blocks, encrypting them, generating a hash value for every, concatenating it and generating a signature on that. The TPA performs the main role of knowledge integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on that. It later compares each the signatures to verify whether or not the information stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. To make sure data protection or security of cloud data storage at cloud end, security architecture is designed that secures the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of EC-RSA, AES algorithm and Blowfish algorithm along with SHA-256 for auditing purpose. Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency about 40% in terms of execution time i.e. encryption as well as decryption time and security and providing confidentiality of cloud data at could end.**

Keywords - Cloud Computing, Security, Integrity, Confidentiality, TPA, EC-RSA, AES, Blowfish..

I. INTRODUCTION

Cloud computing provides nearly "infinite" and "ubiquitous" data service for cloud users. Among all the services provided by cloud computing, cloud storage is one in all the foremost necessary services that permits cloud users to migrate their knowledge from local storage systems to the cloud [1].

Cloud storage service brings important advantages to knowledge owners, say, (1) reducing cloud users' burden of storage management and equipment maintenance, (2) avoiding investment a large amount of hardware and software, (3) enabling the information access independent of geographical position, (4) accessing data at anytime and from any place. Because cloud storage offers scalable, pay as you go and location independent storage services for cloud users, it's become a fast profit growth point in cloud computing [2].

However, cloud storage will trigger some new security threats to data owners. A number of cloud users wouldn't prefer to use cloud storage because of some serious security worries. A primary concern of cloud users is that the integrity of their outsourced files. There are many factors that may cause data corruption. First, cloud service suppliers aren't totally trustworthy. As a result, for financial reason, the cloud service provider may delete the data that are rarely or have not been accessed in order that it will save the area for storing alternative files for charging extra expenses. Second, the keep knowledge can be corrupted owing to cloud server's failure, management errors or adversary attacks. More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment it is? Issues of cloud computing [3] can summarize as follows:

Data security: In any web based applications, data is often processed in plaintext. Similarly in SaaS, user data security is of prime concern. The SaaS provider is responsible for the data security while processing and storing it at cloud server.

DOI: https://doi.org/10.24113/ojsscience.v3i10.148

Also, in case of disaster or damage, data backup is a critical issue in order to facilitate recovery [4].

Malicious Insiders: Malicious insiders are the threat which can access data or information being a member of the organization. As application data of cloud user is stored on cloud storage provided by cloud provider, malicious insiders can also access to such data.

Data Loss/Leakage: Deletion, stealing or alteration of data and loss of encoding key gives accessing rights to the unauthorized users. Unauthorized access into cloud can leads to data theft and losses.

Information Security: A communication is established between client and server to exchange services between them. A secure communication is to be established for data or application security. Secure communication issues include those security concerns that arise during the communication between client and server. These include issues such as confidentiality, authentication and integrity [5].

Cryptography is a method of achieving security by changing readable form of data into unreadable form. Using cryptography [6] we can protect the sensitive data in network. In cryptography the sensitive data of the user are encrypted in cipher text which adds a security level over the data. This paper motivates the public auditing system of data storage security in Cloud Computing and provides a privacy-preserving auditing protocol, i.e., proposed scheme enables an external auditor to audit user's outsourced data in the cloud without learning the data content [7].

To the best of our knowledge, proposed scheme is the first to support scalable and efficient public auditing in the Cloud Computing. Proposed scheme proves the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

II. RELATED WORK

Wang et al. [4] has planned a privacy preserving public auditing protocol that makes use of an independent TPA to audit the information. It utilizes the public key primarily based homomorphic linear authenticator (HLA) with random masking techniques. However this protocol is susceptible to existential forgeries called message attack from a malicious cloud server and an outside attacker.

To beat this downside, Wang et al. [5] planned a new improved theme that is safer than the protocol planned. It's a public auditing scheme with TPA, that performs data auditing on behalf of users. It uses HLA that is made from Boneh-Lynn-Shacham short signature referred as BLS signatures. It conjointly uses random masking for data hiding. For the sake of data binding, this new theme involves computationally intensive pairing operation so making it inefficient to use. This planned theme has been enforced much on Amazon EC2 instance that demonstrates the quick performance of the planning on each the cloud and also the auditor side. However the full-fledged implementation of this mechanism on commercial public cloud isn't been tested. Therefore it's difficult to expect it to robustly deal with terribly large scale information.

Meenakshi et al. [6] has planned a protocol that uses TPA to audit the information of the users using Merkle Hash Tree algorithmic rule. It supports data dynamics however fails to supply confidentiality to the information hold on within the cloud.

Tejaswani et al. [7] has achieved integrity of knowledge using a Merkle hash tree by TPA and also the confidentiality of knowledge is achieved using RSA primarily based cryptography formula whereas Jadhav et al. [8] have introduced an attacking module that endlessly keeps track on data alteration within the cloud. The attacking module may be a little code that resides on cloud server. Confidentiality of hold on information is achieved by encrypting the information using AES formula.

Arasu et al. [6] has planned a technique that uses the keyed Hash Message Authentication Code (HMAC) with homomorphic tokens to enhance the security of TPA. It's a way for confirming the integrity of a data transmitted between 2 parties that agree on a shared secret key. HMAC's are based on a key that's shared between the 2 parties, if either party's key's compromised, it'll be possible for an attacker to make fraud messages.

Ashutosh Kumar Dubey et al. [10] devised two way secure cloud architecture. The first part is controlled by the normal user where the data is encrypted using RSA algorithm and uploaded into the cloud environment. In the second part, the admin can update the data in the cloud environment by requesting the secure key from the cloud user.

Vishwanath S Mahalle et al. [11] suggested a hybrid approach which uses RSA and AES [9] algorithms providing data security to the user in cloud. In this approach three keys are used. Public key for encryption and private and secret keys for decryption processes. These three keys are used, since it is a combination of Symmetric and Asymmetric algorithms.

D.I. George et al. [12] discusses about the usage of prime numbers instead of random numbers in the proposed system as it improves the speed of encryption and decryption. This speed is still enhanced in the proposed algorithm ERSA by dividing the file into several blocks. Apart from increasing the speed, the implementation of ERSA algorithm also makes the computation complex one and increases the strength of security.

G.Prabu kanna et al. [13] proposed a novel identity based hybrid encryption (RSA with ECC) to enhance the security of outsourced data. In this approach sender encrypts the sensitive data using hybrid algorithm. Then the proxy re-

DOI: https://doi.org/10.24113/ojsscience.v3i10.148

encryption is used to encrypt the keyword and identity in standardize toward enrichment security of data.

Akshita Bhandari et al. [14], proposed framework can protect data while transferring, sharing and storing in data centers using classification of data, Hashed Message Authentication codes and Index Building. The data is divided into three sections and accordingly the user is asked for authentication. User is provided the digital signature which can be verified with cloud directory. Using indexing, search can be made on the encrypted data.

Khalid El Makkaoui et al. [15], proposed a new fast variant of the Cloud RSA scheme to speed up its algorithms. The proposed variant uses a modulus of the form N = prqs for r,s≥2 and employs Hensel lifting and Chinese remaindering to decrypt. Simulation results show that the proposed variant gives a large speed up over the Cloud RSA scheme while preserving a prescribed security level.

R.Swathi et al. [16] proposed an approach named enhancing data storage security in cloud using Certificate less public auditing scheme which is used to generate key value. Key Generation Center (KGC) will generate only the partial key so that at any case it will not compromise user’s private key. Private & public key is generated based on the partially generated private key by the KGC and to check the cloud data reliability of the user’s uploads the data in server and then during the auditing of the reliability of data is checked. Once after checking it then sends the report to the users’. To confirm the data reliability during the auditing process &the server generates the proof and randomly selects the blocks. The TPA then authenticates the proof against cloud server & the auditing result is sent to the user.

III. PROPOSED METHODOLOGY

There is a need to develop an effective public auditing protocol which overcomes the limitation of the existing auditing scheme. The proposed system is developed to verify the correctness of cloud data by TPA, periodically or on demand without retrieving the entire data or without introducing additional online burden to the cloud users and cloud servers. The data owner or the user is responsible for splitting the file into blocks, encrypting those using encryption algorithm, generating a hash value for each, concatenating the hashes on it. The cloud server is used to store the encrypted blocks of files. When the client or data owner request for data auditing to the TPA, it immediately request for the encrypted data from the cloud server. After receiving the data, it generated the hash value for each block of encrypted files.

A. Proposed Algorithm

Step 1: Input data

Step 2: Encrypt data using EC-RSA

Step 3: Generate Hash code using SHA-256 algorithm

Step 4: Send data to the cloud server.

Step 5: Divide the encrypted data into two halves

Step 6: Re-encrypt first half using AES algorithm and second half using Blowfish algorithm

Step 7: Save both data at different cloud server

Step 8: If user wants to decrypt data or wants to audit data

{ Data owner send request to TPA

Cloud Server decrypt data using AES and Blowfish and send to TPA

TPA generates hash code on encrypted data and send the audit report to data owner.}

Step 9: Data owner re-decrypt the data using EC-RSA algorithm.

Step 10: Exit

The main objective of the proposed work is the security concern associated with data files at the Cloud End. In order to keep securities at cloud storage following skeleton of the proposed work which is hybrid in nature containing three stages is given.

The proposed work (as shown in Fig 1) consists of three stages. In first stage, encryption of user’s data using EC-RSA algorithm. The hash value of encrypted data is generated using SHA-256 and send to the Third Party Auditor (TPA). Then encrypted data is sent to cloud server for storage purpose. Further the encrypted file or data is divided into two blocks and re-encrypted by cloud server using AES and Blowfish algorithm respectively and saved at different location at cloud server.

DOI: https://doi.org/10.24113/ojsscience.v3i10.148

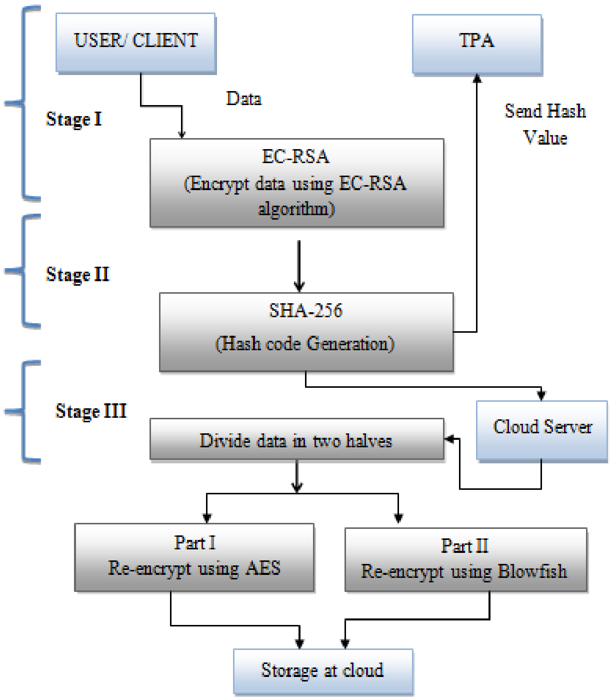
USER/ CLIENT
TPA
Stage I
Data
Send Hash Value
EC-RSA (Encrypt data using EC-RSA algorithm)
Stage II
SHA-256 (Hash code Generation)
Stage III
Cloud Server
Divide data in two halves
Part I Re-encrypt using AES
Part II Re-encrypt using Blowfish
Storage at cloud

Figure 1: File Storage Process

Detailed steps of File Storage Process are described as below:

- Start
- Apply EC-RSA on user data
- Hash value Generation using SHA algorithm
- Server also sends hash value of the password.
- Send to cloud server.
- Data division in two equal blocks.
- Re-encryption of each block using AES and Blowfish respectively.
- Data storage at cloud server.

File retrieval process is also termed as decryption of data file from cloud data center. When a user wants to access his data file that is saved at data center, then first of all he has to authenticate himself at authority server. For this Authority server has to send user ID and password. After authentication of user the server decrypt the data file stored at data server. After decryption of data hash value is matched by TPA over encrypted data. Then finally data and audit report is send to data owner and re-decrypt the data using EC-RSA algorithm. In this way whole process of file retrieval is proceeded and shown in Figure 2.

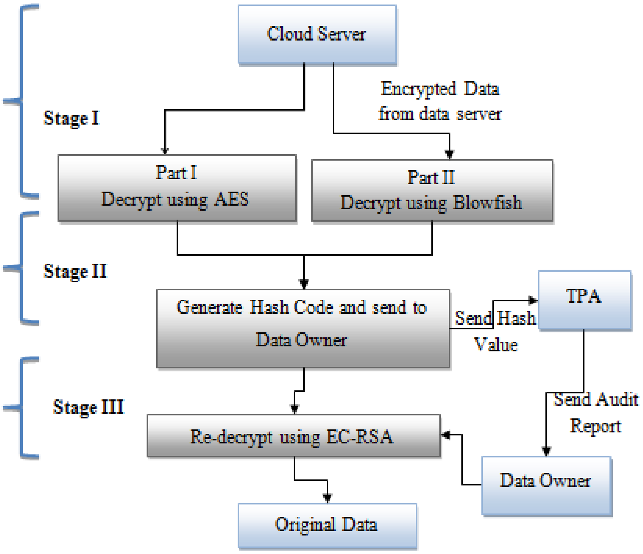

Figure 2: File Retrieval Process

Detailed steps of File Retrieval Process are described as below:

- Start
- Send request to cloud server for data retrieval
- Cloud server retrieve data from the data storage and decrypt divided data block using AES and Blowfish algorithm respectively.
- Hash value matching by TPA.
- TPA sends the audit report to the data owner.
- Data owner re-decrypt using EC-RSA algorithm and retrieve original data block.

IV. RESULT ANALYSIS

For evaluation of performance of proposed algorithm the parameters or criteria is to be determined to analyze or test its efficiency. Here the execution time is preferred factors to analyze the performance of the proposed algorithm to encrypt/decrypt data blocks of various sizes. The table 1, 2 and 3 shows the execution time observation of encryption process and decryption process of proposed algorithm respectively.

Table 1: Hashing Time Performance Evaluation

File size	Hashing Time
49 KB	0.004553
59 KB	0.004937
100 KB	0.008228
247 KB	0.01007

The table 1 shows the hashing time observation of proposed algorithm. Execution process is evaluated using different file size such as 49 KB, 59KB, 100 KB and 247 KB.

Table 2: Encryption Time Performance Evaluation

File Size	ECC	Blowfish	Hybrid two tier	Propose d

DOI: https://doi.org/10.24113/ojsscience.v3i10.148

49 KB	62	34	62.3	12.924
59 KB	66	36	66.5	15.036
100 KB	71	37	71.4	26.263
247 KB	99	45	99.8	63.134
321 KB	102	45	102.9	77.315

The table 2 shows the encryption time observation of proposed algorithm. Execution process is evaluated using different file size such as 49 KB, 59KB, 100 KB and 247 KB.

After analyzing all data files on both existing and proposed algorithm, it is concluded that as data file size increases, execution time for encryption process increases. Figure 3 is showing the analysis of encryption time of proposed algorithm as compared with existing algorithm.

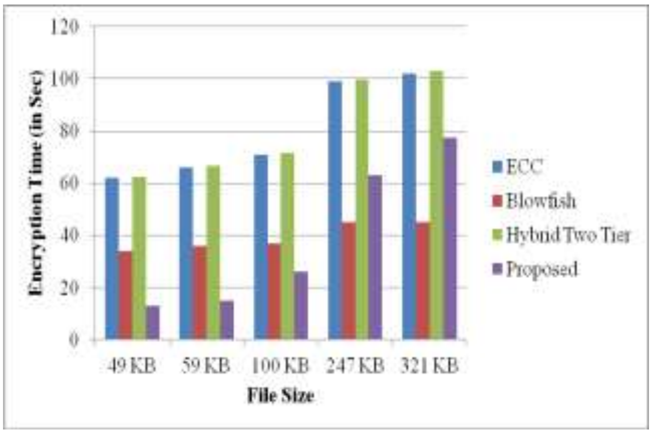

Figure 3: Encryption Time Performance Evaluation

Table 3 is showing the analysis of decryption time of proposed algorithm as compared with existing algorithms

Table 3: Decryption Time Performance Evaluation

File Size	ECC	Blowfish	Hybrid two tier	Propose d
49 KB	25	38	25.3	14.855
59 KB	26	26	26.4	17.269
100 KB	39	52	39.8	26.268
247 KB	103	66	103.4	61.53
321 KB	116	92	116.8	91.381

Decryption process is evaluated using different file size such as 49 KB, 59KB, 100 KB and 247 KB.

After analyzing all data files on both existing and proposed algorithm, it is concluded that as data file size increases, execution time for decryption process increases. But it is also observed that as file size increases, the execution time for decryption process in existing technique increases than proposed algorithm.

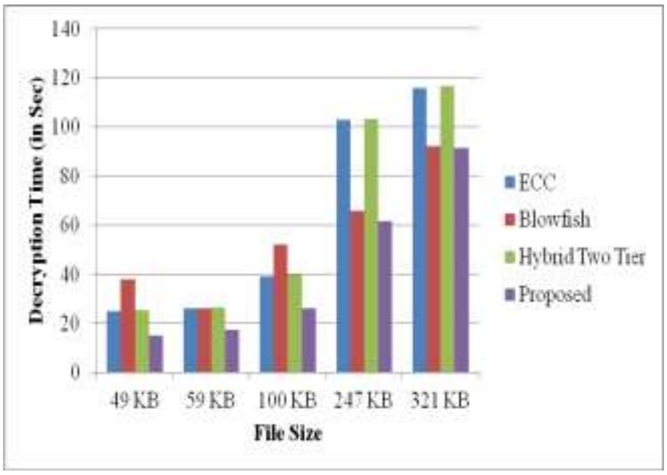

Figure 4: Decryption Time Performance Evaluation

V. CONCLUSION

In order to take care of integrity and confidentiality of user's data at cloud finish there is would like of economical and secure public auditing scheme. A secure and efficient privacy preserving public auditing scheme is been planned that effectively by maintaining every the integrity and confidentiality of information. It achieves privacy preserving and public auditing for cloud by employing a TPA (Third Party Auditor), that will the auditing while not retrieving the data copy, therefore privacy is preserved. The data is hold on within the encrypted format within the cloud storage, so maintaining the confidentiality of information. The data integrity is verified by TPA for the asking of the client by validating both the signatures. It solely checks whether or not the hold on data is tampered or not and informs concerning it to the user. An attempt is created to overcome the restrictions of the prevailing auditing scheme. Presented research work focused on the cloud data protection or security at cloud end. To make sure data protection or security of cloud data storage at cloud end, security architecture is designed that secures the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of EC-RSA, AES algorithm and Blowfish algorithm along with SHA-256 for auditing purpose.

Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency about 40% in terms of execution time i.e. encryption as well as decryption time and security and providing confidentiality of cloud data at could end. This research work also uses the concept of authentication of the user by the concept of SHA-256. The proposed method provides a secure framework for confidentiality of text information at cloud storage data that can be useful in a number of applications at cloud end. Benefits to the proposed technique include the simplicity and confidentiality. A future improvement to the method could

DOI: https://doi.org/10.24113/ojsscience.v3i10.148

be a mechanism to process secure data sharing among different cloud users.

REFERENCES

[1] Mell, Peter, and Tim Grance. The NIST definition of cloud computing, 2011.

[2] Zissis, Dimitrios, and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation computer systems, 2012, pp. 583-592.

[3] Cong Wang, Sherman SM Chow, Qian Wang, Kui Ren, and Wenjing Lou. Privacy Preserving Public Auditing for Secure Cloud Storage. Computers, IEEE Transactions, 2013, pp. 362–375.

[4] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou. Toward secure and dependable storage services in cloud computing. Services Computing, IEEE Transactions, 2012, pp. 220–232.

[5] IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA. International Journal of Advanced Research in Computer Science & Technology (IJARCST), 2014.

[6] Tejaswini, K. Sunitha, and S. K. Prashanth. Privacy Preserving and Public Auditing Service for Data Storage in Cloud Computing. Indian Journal of Research, 2013.

[7] Jadhav Santosh and B.R Nandwalkar. Privacy Preserving and Batch auditing in Secure Cloud Data Storage using AES. Proceedings of 13th IRF International Conference, 2014.

[8] S Ezhil Arasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. International Journal of Recent Technology and Engineering (IJRTE), 2013.

[9] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", IEEE, pp. 1-8, 2016.

[10] Vishwanath S. Mahalle, Aniket K. Shahade, "Enhancing the data security in Cloud by implementing Hybrid (RSA & AES) Encryption Algorithm", IEEE, pp. 146-149, 2016.

[11] D.I. George Amalarethinam, H. M. Leena, "Enhanced RSA Algorithm with varying Key Sizes for Data Security in Cloud", IEEE, 2016.

[12] G.Prabu kanna and V.Vasudevan, "Enhancing the Security of User Data Using the Keyword Encryption and Hybrid Cryptographic Algorithm in Cloud", IEEE, pp. 3688-3693, 2016.

[13] Akshita Bhandari, Ashutosh Gupta, Debasis Das, "A framework for Data Security and Storage in Cloud Computing", IEEE, 2016.

[14] Khalid El Makkaouia, Abderrahim Beni-Hssaneb, Abdellah Ezzatia, Anas El-Ansari, "Fast Cloud RSA Scheme for Promoting Data Confidentiality in the Cloud Computing", Procedia Computer Science, pp. 33–40, 2017.

[15] R.Swathi and T.Subha, "Enhancing Data Storage Security in Cloud using Certificateless Public Auditing", IEEE, pp. 348-352, 2017.

[16] Rodrigo N. Calheiros, Rajiv Ranjan, Anton Beloglazov, C′esar A. F. De Rose and Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", Wiley Online Library, 2010.