A Novel Framework for Secure Cloud Storage Using Biometrics Authentication and Visual Cryptography

[1]Dr. Labisha R.V, [2]Kavya Krishna S.L

[1]Assistant Professor, [2]PG Scholar
Department of Computer Science and Engineering,
Marthandam College of Engineering and Technology, Kuttakuzhi

***Abstract*: Using cloud storage services, users can store their data in the cloud to avoid the expenditure of local data storage and maintenance. To ensure the integrity of the data stored in the cloud, many data integrity auditing schemes have been proposed. In most, if not all, of the existing schemes, a user needs to employ his private key to generate the data authenticators for realizing the data integrity auditing. Thus, the user has to possess a hardware token (e.g. USB token, smart card) to store his private key and memorize a password to activate this private key. If this hardware token is lost or this password is forgotten, most of the current data integrity auditing schemes would be unable to work. The proposed system uses biometric data (e.g. iris scan, fingerprint) as the user's fuzzy private key to avoid using the hardware token. It introduces Encryption and Decryption using fuzzy logic and (n, n) secret shares using fuzzy logic. The meaning of fuzzy is vague, ambiguous and uncertain. Encryption and decryption methods using fuzzy logic will be difficult to guess. Hence secret sharing concept using fuzzy logic is better and enhanced method of encoding of data for more security. Visual cryptography is a technique of encryption to embed secret messages in an original image therefore the secret messages can be decrypted by the human view with requiring not much calculation. The (n, n) secret hiding scheme provides more security and confidentiality. In secret hiding, share images are constructed based on fuzzy logic and user desired input. The (n, n) secret sharing scheme divides information into n shares. During decryption the n shares are brought together recreate the secret information.**

***Keywords*: Cloud, Biometrics, Secret Shares**

1. INTRODUCTION

Cloud computing is an information technology paradigm, a miniature for enabling everywhere to get the shared configurable resources which can be immediately vend with minimum authority creation, usually over the internet. Cloud computing allows users and business with different computing potential to store and process data either in a private cloud or on a public cloud. There will be a third party also in the data center. Thus, how the cloud makes the data access function more dynamic and significant. With the sharing of the resources the cloud computing achieves the economic scale and the coherence. The cloud users get number of assets from the Cloud computing. Users expense for the CAPEX is almost negligible while software and service charge will vary as per the usage. The user can access wide range of applications and data immediately where ever they have a network. Cloud computing applications extent over in many domains like social networks, life science, health care, business, data analytics etc. The users are still facing the problem over the data integrity both in the internal and external within large area. The growth in the cloud computing with in infrastructure where the cloud service providers provision the computing and storage resources to their clients or business, to provide integrity guarantees for outsourced data management will be the significant importance. The tremendous problem relates with the untrusted servers provide data integrity verification in cloud data storage. The useful techniques of security in cloud storage is to verify data integrity stored in public cloud is (cloud storage auditing). This sytem design a practical data integrity auditing scheme without private key storage for secure cloud storage. In this scheme, two fuzzy private keys (biometric data) are extracted from the user in the phase of registration and the phase of signature generation. The proposed system respectively use these two fuzzy private keys to generate two linear sketches that contain coding and error correction processes. In order to confirm the user's identity, compare these two fuzzy private keys by removing the "noise" from two sketches. If the two biometric data are sufficiently close, it can confirm that they are extracted from the same user; otherwise, from different users. How to design a signature satisfying both the compatibility with the linear sketch and the block less verifiability is a key challenge for realizing data integrity auditing without private key storage.

II. RELATED WORKS

S. G. Worku et.al proposes a privacy preserving public auditing scheme that supports public auditing and identity privacy on shared data stored in the cloud storage service for enhancing its security and efficiency.

Y. Yu et al., introduces a new construction of identity-based (ID-based) RDIC protocol by making use of key-homomorphic cryptographic primitive to reduce the system complexity and the cost for establishing and managing the public key authentication framework in PKI-based RDIC schemes.

Y. Zhang, J. et al., propose a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation and a new private key update technique.

W. Shen, J. et al.,proposes a novel storage auditing scheme that achieves highly-efficient user revocation independent of the total number of file blocks possessed by the revoked user in the cloud. This is achieved by exploring a novel strategy for key generation

and a new private key update technique. Using this strategy and the technique, it realize user revocation by just updating the nonreworked group users' private keys rather than authenticators of the revoked user.
H. Jinet al., proposes a public auditing scheme with data dynamics support and fairness arbitration of potential disputes.
Y. Zhu, H. et al., proposes a dynamic audit service for verifying the integrity of untrusted and outsourced storage. The audit service, constructed based on the techniques, fragment structure, random sampling it can support provable updates to outsourced data, and timely abnormal detection.

III. PROPOSED SYSTEM

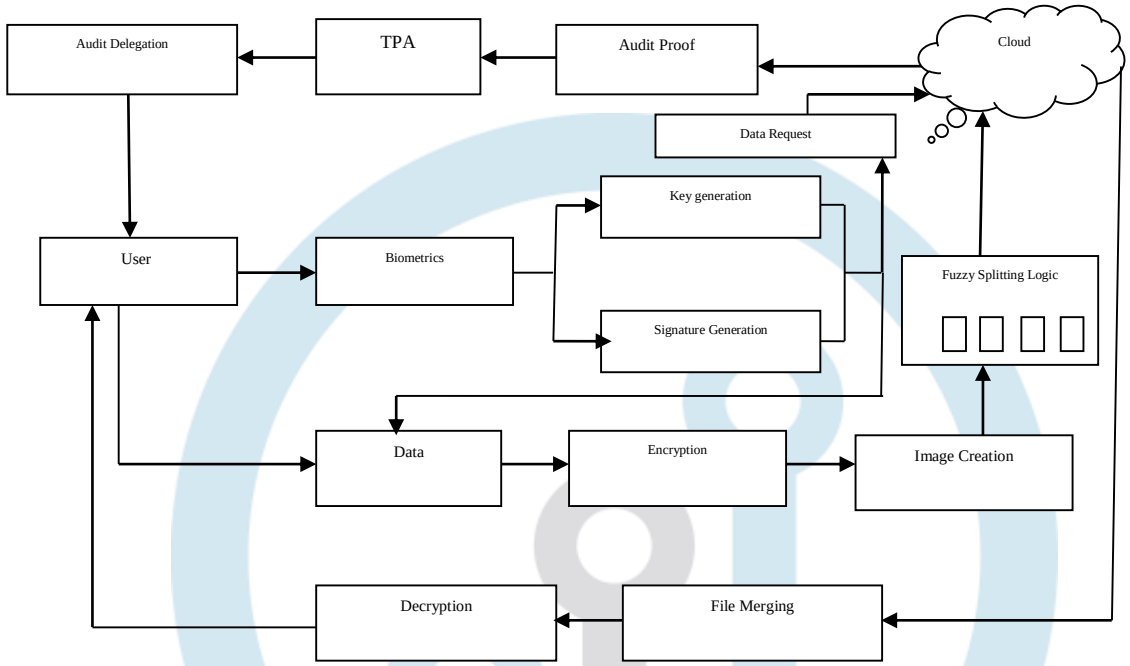

Figure 2: Block Diagram

IV. CONTRIBUTION

The system model involves three types of entities: the user, the cloud, and the TPA. The cloud provides enormous data storage space to the user. The user has a large number of files to be uploaded to the cloud. The TPA is a public verifier who is delegated by the user to verify the integrity of the data stored in the cloud. In the phase of user registration, the biometric data (e.g. fingerprint) is extracted from the user who wants to use the cloud storage service. When a data owner would like to upload data to the cloud, he firstly extracts biometric data as his fuzzy private key and randomly generates a signing key. Then, this data owner computes authenticators for data blocks with his signing key. Finally, he uploads these data blocks along with the authenticator set to the cloud and deletes these messages from the local storage.

A. User

The cloud provides enormous data storage space to the user. The user has a large number of files to be uploaded to the cloud. The TPA is a public verifier who is delegated by the user to verify the integrity of the data stored in the cloud. In the phase of user registration, the biometric data (e.g. fingerprint) is extracted from the user who wants to use the cloud storage service. When a data owner would like to upload data to the cloud, he firstly extracts biometric data as his fuzzy private key and randomly generates a signing key. Then, this data owner computes authenticators for data blocks with his signing key. Finally, he uploads these data blocks along with the authenticator set to the cloud and deletes these messages from the local storage.

B. Signature Generation

The concept of fuzzy signature uses biometric data as private key, such as iris scan and fingerprint, to generate the signature. The biometric data y is a feature vector which is defined as an n-dimensional vector. In a fuzzy signature scheme, the key generation algorithm KeyGen takesthe biometric data y as input, and generates a verification key vk. The signature generation algorithm SigGen takes as input the biometric data y' and a data block mi, and generates the signature of mi. The verification algorithm Verify takes as input the verification key vk, the data block mi and the signature and verifies whether the signature is valid or not. If the biometric data y' is sufficiently close to the biometric data y, it means that y0 and y are extracted from the same user. Thus, the signature is valid; otherwise, it is invalid.

Specifically, the data owner randomly generates a signing key sk' and its corresponding verification key vk', where sk' is used to generate the sketch and the authenticators. Then the data owner generates a sketch c' of signing key sk' using the biometric data y' extracted from him. He generates a data authenticator set for file F with signing key sk'. The signature of file F is (ϕ, vk', c'). The data owner sends file to the cloud, and deletes them from the local storage. The Proof Gen algorithm and Proof Verify algorithm are executed in this phase.

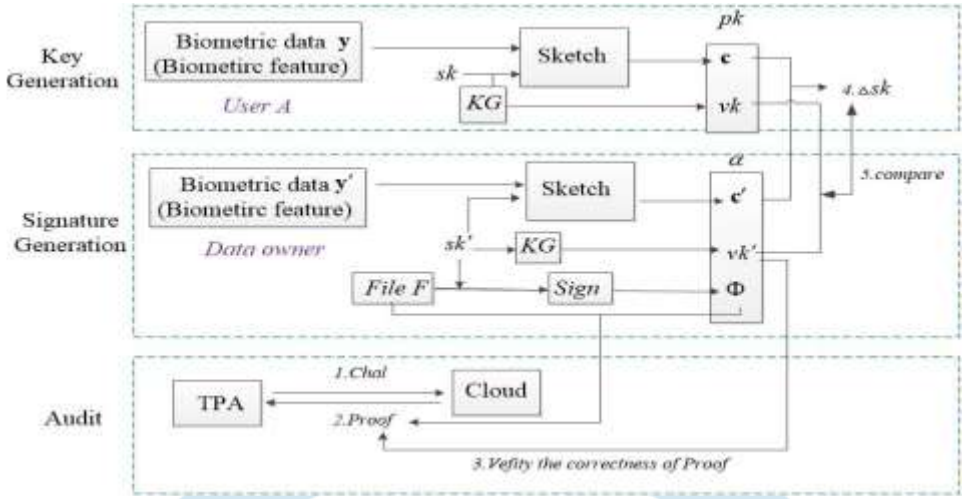

Fig 2 : Signature Generation

C. Encryption

The Encryption plot utilizes AES calculation for encryption of documents. AES utilized as a part of our paper is of 128 bits, 192 bits, 256 bits. At the point when the client presents its document alongside the secret word then the encryption conspire calls the fluffy rationale to get the AES encryption bits (128,192,256). At that point it calls the encryption key generator to create a key of the required bits. After that the encryption conspire begins the encryption procedure. In this strategy, it's exceptionally troublesome for the aggressor to know which bit AES was performed. Additionally the key age depends on randomization so it's difficult for assailant to know the key.

D. Visual Cryptography

A (n, n) visual mystery concealing plan produces n shares pictures from a scrambled picture and including n shares together gives an encoded picture. The (n, n) visual mystery sharing plan partitions the mystery picture or record content into n shares so reproduction of mystery picture or document content from an offer is unimaginable. Here in (n, n) visual mystery sharing plan, it isolates the mystery picture or record content into n shares. For instance a mystery picture is to be shared among two members since it is (n, n) mystery concealing plan. The picture is isolated into n shares with the goal that when n shares are included it is unmistakable. At the point when not as much as n shares are included, the mystery stays undetectable.

E. Decryption

Decoding is the strategy for changing over information that has been gotten confused through encryption process back to its plain content frame. In decoding, the framework concentrates and changes over the data and changes it to writings and pictures that are effectively justifiable by the framework and the peruser too. The Decryption procedure does decoding on the collector side. The Decryption technique recovers the first mystery picture from created shares. The offers containevery one of the points of interest which are expected to begin the unraveling procedure. The scrambled offers are recovered and after that in view of the keythe procedure begins. Thus the first picture or document is downloaded on the beneficiary end.

F. Auditing

The Proof Gen algorithm and Proof Verify algorithm are executed in this phase. In the Proof Gen algorithm, the TPA sends an auditing challenge chal to the cloud. Upon receiving the chal, the cloud returns an auditing proof P to the TPA. In the Proof Verify algorithm, the TPA firstly checks the correctness of the proof P using the verification key vk'. And then, in order to confirm the identity of the data owner, the TPA recovers sk from c and c' by using the technique of coding and error correction. Finally, the TPA verifies whether the difference between vk and vk' truly corresponds to sk. If it does, the data owner is the user A; otherwise, he is not. To verify the integrity of cloud data, the TPA randomly selects a c-element subset I of set [1; s], and generates a random for each i € I. The TPA ends the auditing challenge chal = fi; to the cloud. Upon receiving the auditing challenge, the cloud computes a linear combination of data blocks and an aggregated data authenticator. Then, the cloud returns an auditing proof to the TPA. The TPA checks whether the following equation holds.

$$E(\sigma,g) = e\ (\Pi_{2\epsilon I} H(name||i)^{\beta i}\ .u^{\mu}, vk')$$

If the equation does not hold, then the data stored in the cloud is corrupted; otherwise, the TPA does as follows:
The TPA recovers Δx from c and c' by computing Pw(c – c') = Δx and CRTw(Δx) = Δx, which can confirm the identity of the user. Then, he verifies the following equation holds or not: (vk)zΔx = vk'. If the equation holds, then the data stored in the cloud is intact; otherwise, it is corrupted.

V ALGORITHM

Sender Side

Step 1: Login or Signup

In order to submit the files, login is mandatory. Login helps in identifying the sender and the receiver.

Step 2: Enter confidential data along with password The file is submitted after login along with the password. The password is necessary which is used to generate the key.

Step 3: Fuzzy Encryption Login
The Fuzzy contains some rules and memberships sets which decide the AES bit needs to be performed on the file.

Step 4: Key Generator
The key generator receives a value from fuzzy encryption logic and that based on that it will generate one key from the following bits: 128 bits, 192 bits, and 256 bits.

Step 5: Encryption Algorithm
Encryption is a technique of making an original message unreadable with an encryption algorithm. The encryption algorithm is a combined work of data encryption and decryption process. It provides high security to the information that are transmitted. File is encoded using a secret key.

Step 6: Image Creation
The data from the encrypted file is stored in a blank image. The width and height of image is 256 x 256

Step 7: Fuzzy Splitting Logic
The Fuzzy Splitting Logic is used to generate the range for secret shares. To achieve security from various attackers, the algorithm uses different key variables and values. The user will then choose a value from the derived range.

Step 8: Secret Shares

Based on fuzzy logic and user value the shares of the encrypted image is formed and saved into the internal storage of the server.

Receiver Side
Step 1: Login or Signup
In order to submit the files, login is mandatory. Loginhelps in identifying the sender and the receiver.

Step 2: File Reception
The server will merge the shares and decrypt the file. The receiver will thenable to download the original file.

VI. EXPERIMENTAL RESULTS

We run these experiments on a Windows machine with an Intel Pentium 2.70GHz processor and 4GB memory. Our scheme is implemented by utilizing .net programming language with the GNU Multiple Precision Arithmetic (GMP) Library and the free Pairing-Based Cryptography (PBC) Library. The following are the snapshots of results on execution of the program considering different cases are shown below. The snapshot in figure 2 shows the user registration with biometric data (fingerprint image) and the system generate the signature and secret key to the user. The figure 3 shows the login process, once the user enter the biometrics data the system will automatically generates the signature and secret key which is used for data encryption and decryption. Then the encrypted data is applied with visual cryptography to divide the image into (m,n) secret shares and disturbed the shares in the cloud storage.

Fig 3 : Home Screen

Fig 4 : Registration form

Fig 5 : Login

Fig 6 : Signature and secret key Generation

Fig 7 : File Upload

Fig 8 : File Encryption

VII. CONCLUSION

The proposed system implements the fuzzy private key to realize data integrity auditing without storing private key. The first practical data integrity auditing scheme without private key storage for secure cloud storage. In the proposed scheme, it utilizes biometric data (e.g. fingerprint, iris scan) as user's fuzzy private key to achieve data integrity auditing without private key storage. The proposed system is a mystery document encryption depends on fluffy rationale for mystery message exchange tilizing (n, n) mystery concealing plan. To give the confirmation (n, n) mystery concealing plan is utilized. The information encryption procedure is simple yet information inside picture and afterward picture encryption in view of fluffy rationale and mystery covering up is something else which is exceptionally hard to split. This ordinary system gives greater security, privacy and honesty to the mystery message from unapproved individual.

REFERENCES

[1] A. F. Barsoum and M. A. Hasan, "Provable multicopy dynamic data possession in cloud computing systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 485–497, March 2015.
[2] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015.
[3] H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE Transactions on Cloud Computing, vol. 13, no. 9, pp. 1–14,2014.
[4] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.
[5] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.
[7] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," IEEE Transactions on Information Forensics & Security, 2010 vol. 14, no. 2, pp. 331–346.
[8] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in ACM Symposium on Applied Computing, 2011, pp. 1550–1557.
[9] Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 767–778, April 2017.