Privacy-Preserving Public Auditing For Shared Data on The Cloud

Nitin Tukaram Jagdale[1], Sahil Bashir Tamboli[2], Ashish Kumar[3], Sonali Kale[4]
[1, 2, 3, 4] KJEI's Trinity Academy of Engineering, Pune

Abstract- *With cloud storage services, it is common place for data to be not only stored in the cloud, but also shared across multiple users. However, public auditing for such shared data. while preserving identity privacy remains to be an open challenge. In this paper, we propose the first privacy-preserving system that allows public auditing on shared data stored in the cloud. In particular, we utilize ring signatures to compute the verification information needed to audit the integrity of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private, who is still able to verify the integrity of shared data without retrieving the entire file. Our experimental results demonstrate the effectiveness and efficiency of our proposed mechanism when auditing shared data.*

Keywords - Authentication, Cloud computing, Cryptographic controls, privacy-preserving, shared data.

I. INTRODUCTION

The integrity of data in cloud storage, however, is subject to uncertainty and survey, as data stored in an untrusted cloud can easily be lost or corrupted, due to hardware failures and human errors. To protect the integrity of cloud data, it is best to perform public auditing by introducing a third party auditor , who offers its auditing service with more powerful computation and communication abilities than regular users.

The first provable data possession mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward, Wang et al. is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor. We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the third party auditor, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others.

Cloud computing is an Internet based computing which enables sharing of storage services. The cloud server can store massive data of users and does not ensure data correctness and privacy to cloud users. With the help of cloud technology, the users are able to distribute their data among others. Now a days data sharing becomes a most important feature in many cloud storage services, such an example is Drop box and Google Docs, in which most users relay on cloud storage.

Nowadays the growth of cloud computing environment is encouraging many organizations to migrate their IT infrastructure to function completely or moderately in the cloud. Also cloud computing provides huge number of services on internet to the various users by using large scale data centers, because of their changes in providing being a product to services. Though the cloud supplier guarantees a more secure and dependable environment to their clients, the uprightness of information in the cloud might still be traded off, because of the presence of programming disappointments and human blunders. Thus it is a need to take a time from user's side to check the integrity of the data by performing periodical verifications of their outsourced data.

II. LITERATURE SURVEY

S No	Year	Title	Author	Description
01)	2016	Preserving Privacy in Public Auditing for Shared Cloud Data	Anjali R. S. Department of Computer Science and Engineering	Cloud technology helps the authenticated cloud users to access plenty of resources that are transferred and accumulated in cloud. To preserve the data security and un-authorized users from accessing the users confidential data

				a auditing mechanism can be performed with the help of a third party auditor.
02)	2016	Cloud Based Two Tier Security Scheme for Store, Share and Audit Our Data into Cloud	Ms.Priya Kharmate Department of Computer Engineering	To mitigate the risks of privacy of data stored on cloud with objective of minimum computational overhead and the fact that the data owner cannot always stay online hence the data privacy maintained through auditing process.
03)	2016	Public Auditing Services in Cloud Networks for Data Sharing Including Privacy Preserving	Sonal Shukla Computer Science, Maharishi Ar vind College of Engg. and Reaserch Center, Jaipur, India	This system development demonstrating incorporates three interesting substances: Users that has a great deal of information to be secured in cloud and have the approvals to get to and control set away information. Cloud Service Providers who cording ate to give data stockpiling organizations have sufficient stockpiles and calculation assets
04)	2013	Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics	Boyang Wang State Key Laboratory of Integrated Service Network	In this Project, we propose a privacy-preserving public audit-ing mechanism in the cloud for dynamic groups. By sharing a common group private key with users in the group, each user is able to compute valid signatures on shared data, so that the TPA is able to audit the integrity of shared data for the group but cannot reveal the identity of the signer on each block
05)	2015	Identity-Preserving Public Auditing for Shared Cloud Data	Kai He Computer School, Wuhan University, Wuhan, China	We proposed an identity-preserving public auditing scheme for shared data in cloud storage. By utilizing the idea of proxy re-signatures and the technique of bilinear pairing, our scheme achieves identity preserving against the TPA and the auditing cost is very low.

III. ALGORITHM USED

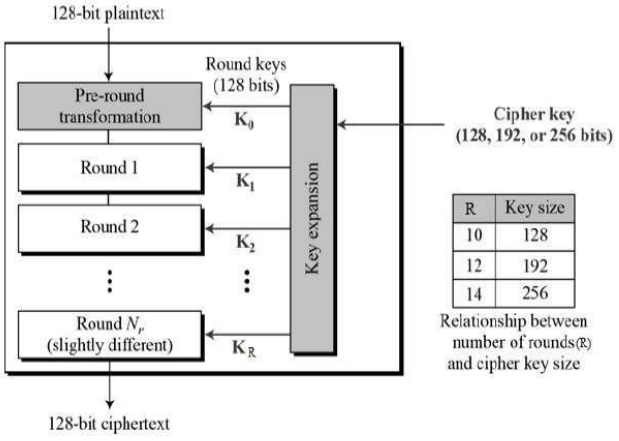
- AES

For encryption of file we are using AES algorithm. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The features of AES are as follows −Symmetric key symmetric block cipher, 128-bit data, 128/192/256-bit keys, Stronger and faster than Triple-DES, Provide full specification and design details. In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

The schematic of AES structure is given in the following illustration –



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

IV. SYSTEM ARCHITECTURE

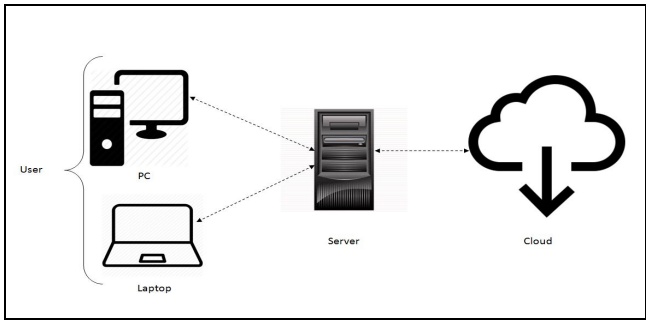


Fig. System Architecture

V. MODULE WORKING

1. Admin Module-

Admin get notification when where user try to change settings then admin will be asked one security question if that answer matches with the database values then admin will allowed change settings.

2. User Module-

1) Login-Registration

Any user before using our system must register with website; user will enter his all personal details and login credentials. Along with personal information user will have to answer one security question which will be used as verification at the time of editing profile. Using same login credentials user have login to application. Due to use of this authentication methodology any unauthorised user cannot use our system because system deals with files sharing and thus we have to secure system.

2) File Upload- Download

When authorised user login to system, he can upload any type of file to system, at the time of uploading file will get encrypted and then get stored to cloud, in our system we are using Hostinger cloud for online storage of files.

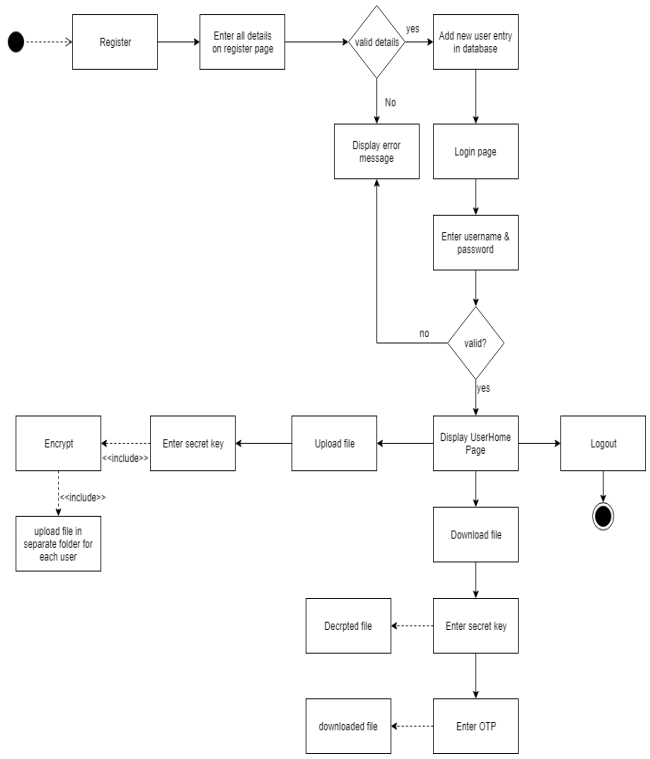


Fig. Module Working

VI. SYSTEM FEATURES

We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. .It implies that the data are stored in one or more servers in the network and that there is some software locking mechanism that prevents the same set of data from being changed by two people at the same time. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless i ntegration of these two salient features in our protocol design. Data sharing is a primary feature of a database management system .They appended the current time period to the ciphertext, and OTP

VII. CONCLUSION

We propose, the first privacy preserving public auditing mechanism for shared data in the cloud. We utilize to construct homomorphic authenticators, so the third party auditor is able to audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor. To improve the efficiency of verification for multiple auditing tasks, we further extend our mechanism to support batch auditing.

VIII. FUTURE SCOPE

- Providing better authentication and allow total group access to shared accounts.
- Providing a better user interface to view shared files
- Extending our app so that it can be used on multiplatform such a iOS, Blackberry OS.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.