International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 6, November-December 2014 ISSN 2278-6856

PRIVACY PRESERVATION AND PUBLIC AUDITING FOR CLOUD DATA USING ASS

Dr. J. SUGANTHI[1], ANANTHI J[2], S. ARCHANA[3]

[1]Professor and Head, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India

[2]Assistant Professor, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India

[3]PG scholar, Department of Computer Science and Engineering
Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract

Cloud computing is a class of network based computing through Internet. Cloud data services stores data in the cloud as well as shares data among many users. The integrity of these cloud data is subjected to reluctance due to failure of either hardware or even software and also human errors as well. Several mechanisms have been designed in order to allow both the data owners as well as the public verifiers to audit cloud data integrity efficiently without retrieving the entire data from the cloud servers. A Third Party Auditor (TPA) will perform integrity checking and the identity of the signer on each block in shared data is kept private from them. In this paper, a privacy-preserving mechanism is designed which supports public auditing on shared data stored in the cloud. In particular, aggregate signatures are used which computes the verification metadata needed to audit the correctness of shared data. With this mechanism, the identity of the owner who signs each data block in shared data is kept private from public verifiers. These public verifiers are able to efficiently verify integrity of shared data without downloading the entire file. In addition, this mechanism can efficiently perform multiple auditing tasks at same time instead of verifying them one by one.

Index Terms:- Public auditing, Shared data, Cloud Computing

1. INTRODUCTION

Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Clouds can be classified as public, private or hybrid. The criticisms about it are mainly focused on its social implications. This happens when the owner of the remote servers is a person or organization other than the user, as their interests may point in different directions, for example, the user may wish that his or her information is kept private, but the owner of the remote servers may want to take advantage of it for their own business. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources [2]. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. Recently, many mechanisms[3][4][5] have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing . In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user (e.g., researcher) who would like to utilize the owner’s data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. [6] designed an advanced auditing mechanism, so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud. We believe that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers [1]. Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information (e.g., which particular user in the group or special block in shared data is a more valuable target) to public verifier. In order to protect the confidential information, it is essential and critical to preserve identity privacy from public verifiers during public auditing. In this paper, to solve the above privacy issue on shared data, a novel privacy-preserving public auditing mechanism is used using Aggregate Signatures to construct homomorphic authenticators so that a public verifier is able to verify the integrity of shared data without retrieving the entire data—while the identity of the signer on each block in shared data is kept private from the public verifier. In addition, this mechanism also supports batch auditing, which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. The remainder of this paper is organized as follows. In Section 2, the system model, context free diagrams and design modules are given. In Section 3, the implementation details are given. In section 4, cryptographic primitives used in Aggregate Signatures are being described. In Section 4, the performance of aggregate signatures is being evaluated. Section 5 gives the Results and Discussions; Section 6 gives the conclusion of the work. Finally, we briefly discuss the future enhancement of the work needed.

2. PROBLEM STATEMENT

2.1 SYSTEM MODEL

The system model in this paper involves three parties: the cloud server, a group of users and a public verifier as shown in fig 2.1. There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed to access and modify shared data. Shared data and its verification metadata are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing services or a data user outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server. When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and- response protocol between a public verifier and the cloud server.

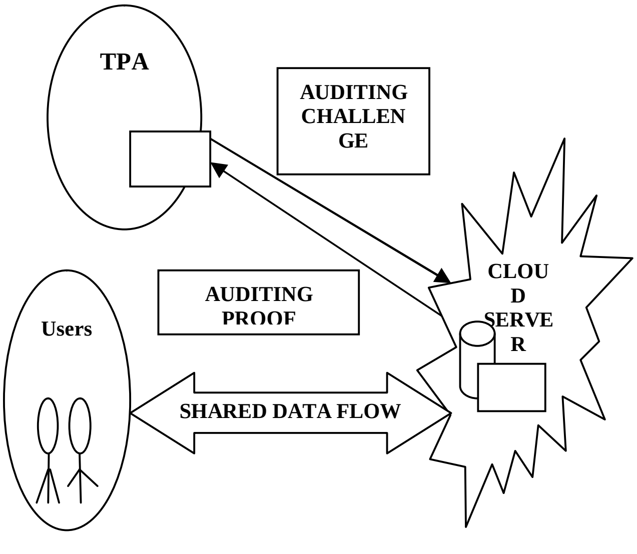


Fig 2.1 System Flow

2.2 FLOW DIAGRAM

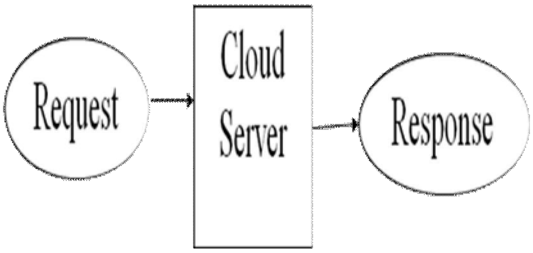


Fig 2.2 Context Diagram

The context diagram shown in Fig 2.2 shows the step by step process taken in the phase of input to output processing of data. This includes the user request and corresponding client- server communication that results in user output. This is accomplished with the use of cloud services wherein the cloud acts as a virtual storage space for storing large amount of data. The request can be from a group of users who may share a common data and uses it efficiently.

3. IMPLEMENTATION

3.1 USERS

Fig 3.1 Cloud Users

A user is a person who can access resources from the cloud. These can be a single person or a group of persons who would share the data available in cloud. Fig 3.1 shows a group of users who shares a single data from a single cloud. For instance, Alice and Bob work together as a group and share a file in the cloud .The shared file is divided into a number of small blocks, where each block is independently signed by one of the two users with existing public auditing solutions. Once a block in this shared file is modified by a user, this user needs to sign the new block using his/her private key. Eventually, different blocks are signed by different users due to the modification introduced by these two different users. Then, in order to correctly audit the integrity of the entire data, a public verifier needs to choose the appropriate public key for each block (e.g., a block signed by Alice can only be correctly verified by Alice’s public key). As a result, this public verifier will inevitably learn the identity of the signer on each block due to the unique binding between an identity and a public key via digital certificates under public key infrastructure (PKI). The user would first register to the interface to get the services. Once the user has registered he/she can log inside the system to get the access of services. Then they can request for the file to the cloud service admin. There will be a third party auditor who performs the integrity checking of the data before providing it to the users. This is done by 1st splitting the data into blocks and then performing integrity check.

The user will get a mail confirmation message which could be a random key generated individually for each file and this is entered in order to access and use the file from the cloud. Hence if the user is not valid he/she is not able to access the file since the randomly generated key is essential for the file access. Once the accessing of file is done by the user, they can efficiently use the file as per wish. This can be limited within a group of persons as well. In a company or organizations say for example, the users can be restricted since there may be confidential data present within the organization. Hence it is very much essential to have random key which is unique for a file.

3.2 THIRD PARTY AUDITOR

Recently, many mechanisms have been used to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking. A public verifier could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. Moving a step forward, Wang et al. designed an advanced auditing mechanism, so that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud.

Sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct. Existing public auditing mechanisms can actually be extended to verify shared data integrity. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers. Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information (e.g., which particular user in the group or special block in shared data is a more valuable target) to public verifiers. After performing several auditing tasks, this public verifier can first learn that Alice may be a more important role in the group because most of the blocks in the shared file are always signed by Alice; on the other hand, this public verifier can also easily deduce that the eighth block may contain data of a higher value (e.g., a final bid in an auction), because this block is frequently modified by the two different users. In order to protect this confidential information, it is essential and critical to preserve identity privacy from public verifiers during public auditing. Third Party Auditor will perform the verification of files by using Aggregate Signature Schemes. After performing the file verification, the result is been updated so that when a user or owner is trying to use a particular file, the status of verification is known to them. The Aggregate Signatures are defined as schemes based on co-GDH signatures. Unlike the co-GDH scheme, aggregate signatures require the existence of a bilinear map.

3.3 CLOUD SERVER

Cloud Servers allows centralizing all the business data and applications into a single cloud server environment. By utilizing the Remote Desktop services on a cloud server, one can allow staff to access their desktop, data and applications from anywhere at any time. Cloud servers eliminate the need for in-house server equipment and network infrastructure, so one can save on IT service costs and take care of critical offsite data protection all at the same time.

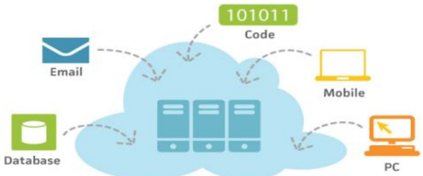


Fig 3.3 Cloud Server

Remote Desktop Cloud Servers can turn the old outdated PC into a powerful remote computing environment providing access to all the latest Microsoft Office software and business applications if there is a stable internet connection. Cloud servers are fully scalable so the possibilities are up to the user. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data. Cloud storage services may be accessed through a co-located cloud compute service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems**.**

4. CRYPTOGRAPHIC PRIMITIVES USED IN AGGREGATE SIGNATURES

An aggregate signature scheme is a digital signature that supports aggregation: Given n signatures on n distinct messages from n distinct users, it is possible to aggregate all these signatures into a single short signature. This single signature (and the n original messages) will convince the verifier that the n users did indeed sign the n original messages (i.e., user I signed message Mi for i = 1,… n). An efficient aggregate signature is constructed from a recent short signature scheme based on bilinear maps due to Boneh, Lynn, and Shacham. Aggregate signatures are useful for reducing the size of certificate chains (by aggregating all signatures in the chain) and for reducing message size in secure routing protocols such as SBGP.

4.1 Aggregate Signature Security

Informally, the security of aggregate signature schemes is equivalent to the nonexistence of an adversary capable, within the confines of a certain game, of existentially forging an aggregate signature. Existential forgery here means that the adversary attempts to forge an aggregate signature, on messages of his choice, by some set of users. We formalize this intuition as the aggregate chosen-key security model. In this model, the adversary A is given a single public key. His goal is the existential forgery of an aggregate signature. We give the adversary power to choose all public keys except the challenge public key. The adversary is also given access to a signing oracle on the challenge key. His advantage, Adv AggSigA, is defined to be his probability of success in the following game.

Setup: The aggregate forger A is provided with a public key PK1, generated at random.

Queries: Proceeding adaptively, A requests signatures with PK1 on messages of his choice.

Response: Finally, A outputs k-1 additional public keys PK2,….., PKk. Here k is at most N, a game parameter. These keys, along with the initial key PK1, will be included in A's forged aggregate. A also outputs messages M1,….., Mk; and, finally, an aggregate signature σ by the k users, each on his corresponding message.

4.2 Aggregate Extraction

This verifiably encrypted signature scheme depends on the assumption that given an aggregate signature of k signatures it is difficult to extract the individual signatures. Consider the bilinear aggregate signature scheme on a group pair (G1,G2). We posit that it is difficult to recover the individual signatures i, given their aggregate, the public keys, and the message hashes. In fact, we posit that it is difficult to recover an aggregate of any proper subset of the signatures. This we term the k-element aggregate extraction problem.

4.3 The Bilinear Verifiably-Encrypted Signature Scheme

The bilinear verifiably encrypted signature scheme is built on the bilinear aggregate signature scheme of the previous section. It shares the key-generation algorithm with the underlying aggregate scheme. Moreover, the adjudicator's public and private information is simply an aggregate signature key pair. The scheme comprises the six algorithms described below:

Key Generation: KeyGen and AdjKeyGen are the same as KeyGen in the co-GDH signature scheme.

Signing, Verification: Sign and Verify are the same as in the co-GDH signature scheme.

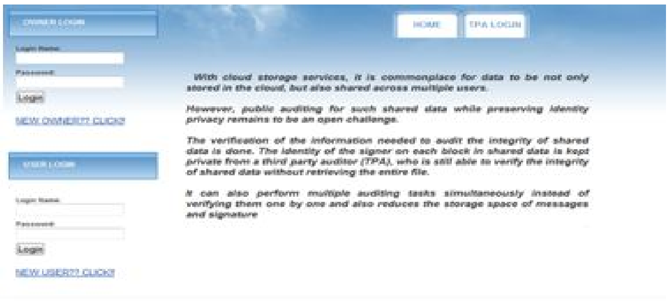
VESig Creation: Given a secret key x, Zp a message M, and an adjudicator's public key v0, compute h and H(M). Select r at random from Zp

VESig Verification: Given a public key v, a message M, an adjudicator's public key v0, and a verifiably encrypted signature, set h and H(M); accept if e(g1, g2) = e(h,v) holds.

Adjudication: Given an adjudicator's public key v0 and corresponding private key x0, a certified public key v, and a verifiably encrypted signature on some message M ensures that the verifiably encrypted signature is valid.

5. RESULT AND DISCUSSION

The screen shots of the work are as given below.



With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users.

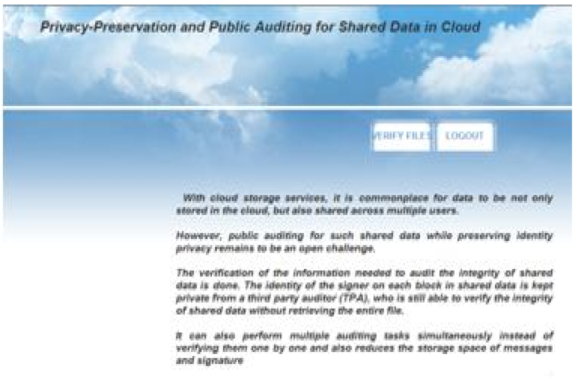
However, public auditing for such shared data while preserving identity privacy remains to be an open challenge.

The verification of the information needed to audit the integrity of shared data is done. The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.

It can also perform multiple auditing tasks simultaneously instead of verifying them one by one and also reduces the storage space of messages and signature

Fig 5.1 Home Page

Fig 5.1 shows the home page of the interface where a new user as well as a new owner can register and log in and also the TPA can perform verification. TPA Login is similar to an admin login and hence no registration is possible for a new TPA to get added and perform security functionalities.



Privacy-Preservation and Public Auditing for Shared Data in Cloud

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users.

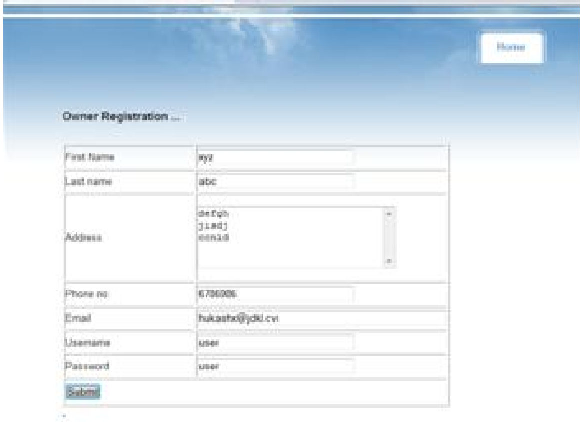
However, public auditing for such shared data while preserving identity privacy remains to be an open challenge.

The verification of the information needed to audit the integrity of shared data is done. The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.

It can also perform multiple auditing tasks simultaneously instead of verifying them one by one and also reduces the storage space of messages and signature

Fig 5.2: TPA Home Page

Fig 5.2 shows the TPA home page wherein the third party auditor will log in and performs verification of files in order to implement integrity of data stored without downloading the entire file.

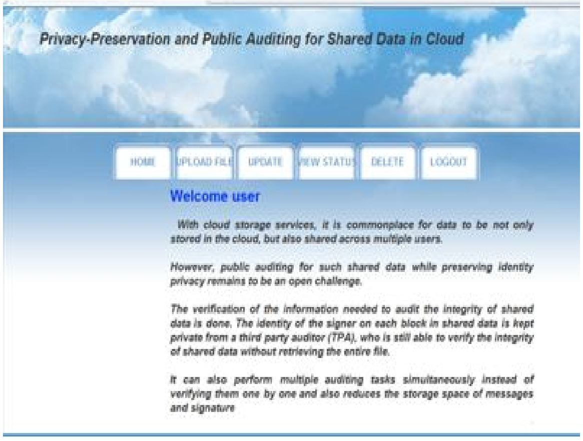


Owner Registration ...

First Name	xyz
Last name	abc
Address	defgh jiadj ccnid
Phone no	6786906
Email	hukashx@jdkl.cvi
Username	user
Password	user

Fig 5.3: Owner Registration Page

An owner who wants to upload some file must first register into the interface. Fig 5.3 shows the registration page of an owner. The details like Name, Address, email ID, username and password are some of the essentials which must be provided.



Privacy-Preservation and Public Auditing for Shared Data in Cloud

Welcome user

With cloud storage services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users.

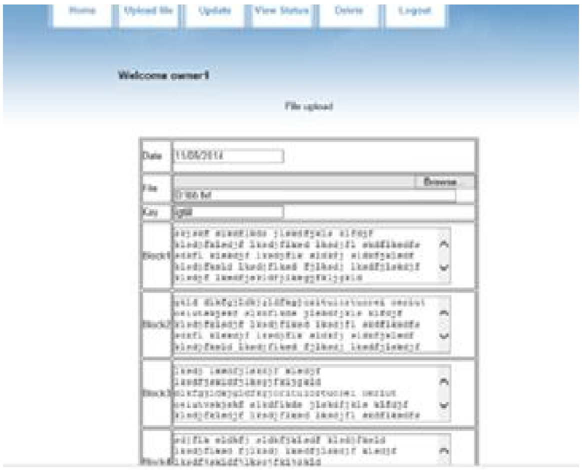
However, public auditing for such shared data while preserving identity privacy remains to be an open challenge.

The verification of the information needed to audit the integrity of shared data is done. The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.

It can also perform multiple auditing tasks simultaneously instead of verifying them one by one and also reduces the storage space of messages and signature

Fig 5.4: Owner Home Page

Fig 5.4 shows the home page of an owner. The owner can perform uploading of a file, updating the file, deleting the file and also can check the status of file verification as well.



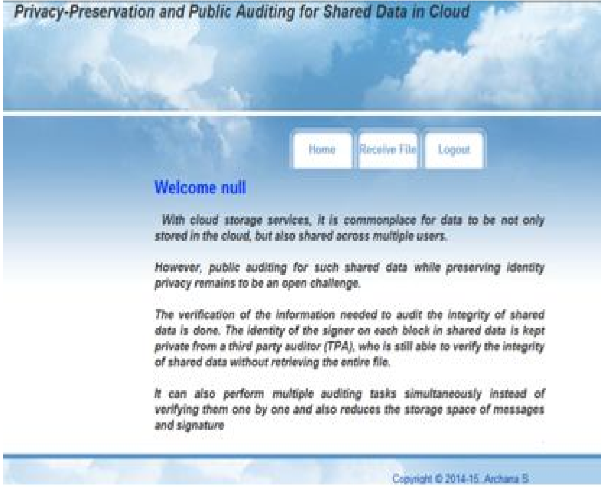
Welcome owner1

File upload

Date	15/08/2014
File	D:\bb.txt
Key	[illegible]
Block1	[illegible]
Block2	[illegible]
Block3	[illegible]
Block4	[illegible]

Fig 5.5: Uploading of file by owner

Fig 5.5 shows an example of an owner uploading a file. The uploaded files are divided into blocks so that a TPA can easily perform verification. A key is generated which is unique for each file.



Privacy-Preservation and Public Auditing for Shared Data in Cloud

Welcome null

With cloud storage services, it is commonplace 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.

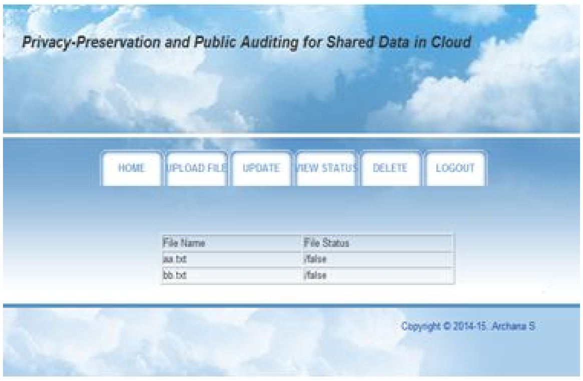
The verification of the information needed to audit the integrity of shared data is done. The identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.

It can also perform multiple auditing tasks simultaneously instead of verifying them one by one and also reduces the storage space of messages and signature

Copyright © 2014-15. Archana S

Fig 5.6: User Home Page

Fig 5.6 shows a User's Home Page wherein a user will login and can request for receiving the files which are being uploaded and verified by owner and TPA respectively.



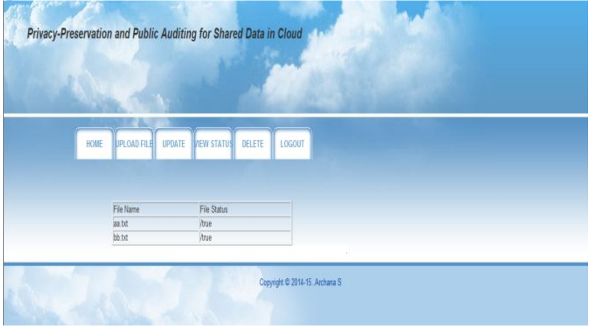
Privacy-Preservation and Public Auditing for Shared Data in Cloud

File Name	File Status
aa.txt	/false
bb.txt	/false

Copyright © 2014-15. Archana S

Fig 5.7: Status of file before TPA verification

Fig 5.7 shows the status of a file before TPA verification. This can be seen by a user as well as by an owner as per request.



Privacy-Preservation and Public Auditing for Shared Data in Cloud

File Name	File Status
aa.txt	/true
bb.txt	/true

Copyright © 2014-15. Archana S

Fig 5.8: Status of a file after TPA verification

Fig 5.8 shows the status of a file after TPA verification. Once TPA verifies a file the update of this verification is made and any owner as well as any user can view this as per request.

6. CONCLUSION

In this paper, we propose, a privacy-preserving and public auditing mechanism for shared data in the cloud. We utilize aggregate signature schemes to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing.

By utilizing Aggregate Signature Schemes the verification and thereby privacy preservation of the data owner is being done and it is seen that the owner could efficiently upload the files and a user could download it using the key which is being sent to his/her mail. The performance and efficiency of the work is valuated.

7. FUTURE WORK

Even though there is greater performance and efficiency in this mechanism, there is a problem of traceability in this system which is been considered to be continued in future work. Since this mechanism is based on aggregate signatures which are group signatures with compressed storage, the identity of the signer is protected. Designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still open. Another problem is data freshness. In future the extension can be done to this ASS mechanism with data freshness in the authenticated file system Also a public batch data integrity auditing protocol for multi-cloud storage can be implemented. In this protocol a third party auditor can simultaneously verify the multiple auditing requests from different users on distinct data files stored on different cloud storage servers.

REFERENCES

[1] B.Wang, B.Li and H.Li, “Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud”, IEEE transactions on cloud computing, vol. 2, no. 1, january-march 2014.

[2] S Archana and Ananthi J, “Privacy-Preservation and Public Auditing for Cloud Data - A Survey”, International Journal of Science and Research (IJSR**),** Vol. 3, No. 10, October 2014, pp-1989-1992.

[3] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, “Aggregate and Verifiably Encrypted Signatures from Bilinear Maps,” Proc. 22nd Int’l Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT’03), pp. 416-432, 2014.

[4] 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.

[5] B. Wang, B. Li, and H. Li, “Public Auditing for Shared Data with Efficient User Revocation in the Cloud,” Proc. IEEE INFOCOM, pp. 2904-2912, 2013.

[6] John W. Rittinghouse James F. Ransome, “Cloud Computing Implementation, Management, and Security”, CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business.

[7].http://ieeexplore.ieee.org/search/searchresult.jsp?queryText%3Dprivacy+in+multiple+cloud&pageNumber=2

AUTHOR PROFILE

Dr. Suganthi J, received her Ph.D in Anna University Coimbatore, TamilNadu, India and is presently working as Director Academic and Head of Department of CSE in Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu, India. She has 13 years of academic and 8 years of industrial experience. She has guided more than 40 UG/PG projects as well as more than 5 research scholars. She has published 2 books and her field of interest is Networking, Data Mining and Image Processing.

Ms. Ananthi J received B.E(CSE) from Government College of Engineering and Technology, Coimbatore in the year 2009 and M.E(CSE) from College of Engineering , Guindy, Chennai in 2011. Presently she is working in Hindusthan College of Engineering and Technology, TamilNadu, India as Assistant Professor in Department of Computer Science and Engineering. She has 3 years of teaching experience. Her research interests are Data Mining and Cloud Computing.

S Archana received the B Tech Degree in Computer Science and Engineering from Jawaharlal College of Engineering and Technology, Palakkad, Kerala, India affiliated to University of Calicut in 2013 and is currently pursuing M.E degree at Hindusthan College of Engineering and Technology, Coimbatore, TamilNadu, affiliated to Anna University. Her field of interest is Cloud Computing and Data Mining.