Enabling secured external auditing process in Cloud Environment

[1]Vaibhav Srikar.M [2]Ezhil Raj.R [3]BeemaMehraj.M

ABSTRACT: **In cloud computing archetype, it is not only used to store the user's data and also allows the users to share the data between them. Sometimes the reliability of the data stored in cloud is lost due to the existence of hardware and software failures and human inaccuracies. To avert these glitches several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the shared data with these existing mechanisms will inexorably disclose confidential details and identity information to public verifiers. In this a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud is proposed. In particular, ring signatures are exploited to compute verification metadata needed to audit the correctness of the shared data. Using this mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who can efficiently verify shared data integrity without retrieving the entire file. In future, this technique will perform multiple auditing tasks simultaneously instead of verifying them one by one.**

KEYWORDS **: Cloud Computing, Privacy-Preserving, Public Auditing , Batch Auditing, Cryptographic Protocols.**

I. INTRODUCTION

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage extents multiple servers and physical environment is typically owned and managed by a hosting company. The cloud storage providers are responsible for keeping the data available and accessible at all times, and the physical environment protected and running. Organizations and individuals buy or lease storage capacity from the providers to store user, organization, or application data. Security of stored data and data in transit may be a concern when storing sensitive data at a cloud storage provider. Users with specific records-keeping requirements, such as public organizations, that must preserve electronic records according to decree, may encounter complications with using cloud computing and storage. When an organization chooses to store data or host applications on the public cloud, it will lose physical access to servers hosting its information. Due to this, potentially business sensitive and confidential data is at the risk of insider attacks. Based on a recent Cloud Security Alliance Report, insider attacks is the third biggest threat to the cloud computing. Therefore, Cloud Service providers must ensure that comprehensive background checks are conducted for employees who have physical access to the servers in the data centre. In addition to that, data centres should be frequently monitored for apprehensive activity.

Cloud computing has been projected as the next generation Information Technology (IT) architecture for enterprises, due to its long list of unmatched advantages in the IT history: on-demand self-service, permeating network access, location independent resource pooling , rapid resource elasticity , usage based pricing and conveyance of risk . From user's point of view, including both individuals and Information Technology enterprises, storage of data remotely to the cloud in a flexible on-demand manner brings alluring benefits like relief from the burden of storage management, universal data access without location dependency, and evasion of capital expenditure on software, hardware, and personnel maintenances, etc. Although, these advantages make cloud computing more luring than ever, it also brings new and challenging security risks towards user's outsourced data. Since cloud service providers are separate administrative bodies, data outsourcing is actually forsaking user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put to jeopardy due to the following reasons.

Examples of security breaches of remarkable cloud services appear quite frequently. Secondly, there exist various motivations for Cloud Service Providers to behave treacherously toward the cloud users regarding their outsourced data status. For examples, Cloud Service Providers might repossess storage for monetary reasons by discarding the data that have not been or been rarely accessed or even hide data forfeiture incidents to maintain their reputation. Objective of this project is to develop and enable privacy-preserving public auditing for cloud data in the cloud storage under the aforesaid model and this protocol design should achieve the following security and performance guarantees Public audit ability, Storage correctness, Privacy preserving, Batch auditing, etc.

II. LITERATURE SURVEY

Cloud computing is one of the long dreamed visions of computing as an utility, where data owners can remotely store their data to enjoy on-demand high-quality applications and services from a shared pool of configurable computing resources. Cloud Computing has been proposed as the next-generation architecture of Information Technology Enterprise. It moves the application software and databases to the centralized and large data centres, where management of the data and services may not be fully reliable. A growing number of online service provider's offer to store customers' photos, email, system backups, and other digital data. Storage outsourcing is an escalating trend which prompts a number of interesting security issues, many of which have been extensively examined in the past[8]. However, Provable Data Possession is a topic that has only recently appeared in the research literature. The main issue is how to efficiently, frequently and securely verify that a storage server is faithfully storing its clients' outsourced data. The storage server is presumed to be untrusted in terms of both security and reliability. Which means it might maliciously or accidentally delete hosted data. It might also relegate it to slow or off-line storage. The problem is aggravated by the client being a small computing device with inadequate resources[8]. Prior work has addressed this problem using the client to outsource its data in encrypted form.

A model for provable data possession (PDP) is introduced [2], which allows a client, who has stored data at an untrusted server to verify that the server possesses the original data without having to repossess it. Probabilistic proofs of possession are generated by the model, by sampling random sets of blocks from the server, which significantly reduces I/O costs. The client maintains a relentless amount of metadata to verify the proof. The challenge and response protocol transmits a small, constant amount of data, which reduces network communication. Therefore, the PDP model for remote data checking supports large data sets in widely distributed storage systems. Two provably secure PDP schemes are presented which are more efficient and effective than previous solutions, even if they are compared to schemes that achieve weaker results.[2] Particularly, the overhead at the server is low or even constant, in contrast to linear in the size of the data. Experiments using this implementation validate the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation. A growing number of online service provider's offer to store customers' photos, email, system backups, and other digital data. [5]Presently, customers cannot make informed decisions about the risk of losing the data stored with any particular service provider, thus reducing their incentive to rely on these services. We argue that the third party auditing is essential in creating an online service oriented economy, because it not only allows customers to evaluate risks but also increases the efficiency of insurance based risk mitigation.[5] We discuss and describe approaches and system hooks that support both internal and external auditing of online storage services, motivations for service providers and auditors to adopt these approaches, and list thee challenges that need to be resolved for such auditing to become a reality. Usually customers use these services to store data such as email, photos, videos, and various other backups. In the present times, a customer must entirely trust such external services to maintain the integrity of hosted data and return it unharmed[3]. Unfortunately, not a single service is foolproof. To make storage services accountable for data loss, Protocols that allow a third party auditor to verify the data stored by a service periodically and assist in returning the data intact to the customer is presented. [3]Most importantly, our protocols are privacy-preserving, which means they never reveal the data contents to the auditor. This solution eliminates the burden of verification from the customer, alleviates both the customers' and storage service's fear of data leakage, and provides a method for independent adjudication of data retention contracts.

While data outsourcing releases the owners of the burden of local data storage and maintenance of the storage, it also removes the owners from having physical control of storage dependability and security, which customarily has been expected by both enterprises and individuals with high service-level requirements[1][4]. In order to aid rapid deployment of cloud data storage service and regain security assurances with outsourced data dependability, effective methods that support on-demand data correctness verification on behalf of cloud data owners have to be designed. [4]This paper proposes that publicly auditable cloud data storage is able to help this nascent cloud economy become fully established and recognized. With public auditability, a reliable entity with expertise and capabilities data owners do not possess can be delegated as an external audit party to assess the risk of outsourced data when in need. An auditing service of such kind not only helps save data owners computation resources but also provides a transparent yet cost-effective method for data owners to gain trust in the cloud.[4] Approaches and system requirements that should be considered, and the outline challenges that need to be resolved for such a publicly auditable secure cloud storage service to become a reality are described. Provable data possession is a technique, used ensure the integrity of data in outsourcing storage service [2].

In this paper, a cooperative provable data possession scheme is considered and proposed in hybrid clouds to support scalability of service and data migration, in which, the existence of multiple cloud service providers to cooperatively store and maintain the clients' data. These experiments show that the verification of our scheme requires a small, constant amount of overhead, which curtails communication complexity. [1]This unique paradigm brings about many new security concerns, which have not been understood well. The problem of ensuring the integrity of data storage in Cloud Computing is studied by this work. Especially the task of allowing a third party auditor, who on behalf of the cloud client, verify the reliability of the dynamic data stored in the cloud is considered. [1]The introduction of Third Party Auditor eradicates the involvement of the client through the auditing of whether his data stored in the cloud is intact or not, which can be important in attaining economies of scale for Cloud Computing.

Support for data dynamics via the general forms of data operation, like block modification, insertion and deletion, is also a noteworthy step toward practicality, because services in Cloud Computing are not limited to archive or backup data only. While works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper accomplishes both. Firstly we recognize the difficulties and potential security glitches of direct extensions with fully dynamic data updates from prior works and then show how to construct an sophisticated verification scheme for the unified integration of these two salient features in the protocol design. Particularly, to achieve efficient data dynamics, the existing proofs of storage models are improved by deploying the classic Merkle Hash Tree construction for block tag authentication. To support effective handling of multiple auditing tasks, the method of bilinear aggregate signature is used to extend the main result into a multi-user setting, by which the Third Party Auditor can perform multiple auditing tasks concurrently. Extensive security and performance analysis show that the proposed schemes are highly efficient and are provably secure.

III. CURRENT ISSUES IN DATA STORAGE AND PUBLIC AUDITING IN CLOUD ENVIRONMENT

The integrity of data in cloud storage is subject to scepticism and scrutiny, as data stored in cloud can be easily lost or corrupted due to the unavoidable hardware and software failures and human errors. The usual approach for checking data correctness is to retrieve the entire data from the cloud. The main reason is that the size of the data stored in cloud is large in general. Downloading entire cloud data to verify data integrity will cost or even waste lot of user's amounts of computation and communication resources, especially when data have been tarnished in the cloud. Recently, many mechanisms have been proposed to allow not only data owner itself but also public verifier to efficiently perform integrity checking without downloading entire data from the cloud, which is referred as public auditing.

IV. PRESERVING PRIVACY IN PUBLIC AUDITING INCLUDING BATCH AUDITING IN ORUTA

To solve the existing privacy issue on shared data a novel privacy preserving public auditing mechanism named Oruta id proposed in this paper. More specifically ring signatures are employed to construct homo-morphic authenticators in Oruta, so that the public verifier can 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 is extended to provide batch auditing, which can accomplish multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks. Our public auditing mechanism includes five algorithms namely **KeyGen**, **SigGen**, **Modify**, **ProofGen** and **ProofVerify**. Using **KeyGen**, users generate their own public and private key pairs. With **SigGen**, a user can compute ring signatures on blocks in shared data by using its own private key and all the public keys of the group members. Any user in the group can perform operations like insert, delete or update on a block, and compute the new ring signature on this new block in **Modify**. **ProofGen** is used by a public verifier and the cloud server together to interactively generate a proof of possession of shared data. In **Proof Verify**, the public verifier by verifying the proof audits the integrity of the shared data.

STEP 1: **Setup Phase**: KeyGen is used by the cloud user to generate the public and secret parameters.

STEP 2: **SigGen**: Given a data file F ={mi }, the user runs SigGen to compute authenticator.

STEP 3:**Audit Phase:** A Third Party Auditor first retrieves the file tag t. Referring to the mechanism we described in the Setup phase, the TPA validates the signature via the secret key, and leaves by emitting FALSE if the Verification fails.

V. MODULES

- **Service Provider**
  - Authentication
  - Resource Provisioning
- **Third Party Auditor**
  - Authentication
  - Auditing Process
- **Data Owner**
  - Authentication
  - Key Maker
  - Auditing Request
- **Data User**
  - Authentication
  - Access Cloud Data

VI. MODULE DESCRIPTION

- **Authentication**

If you are the new user going to consume the service then they have to register first by providing necessary details. After successful completion of sign up process, the user should login into the application by providing username and correct password. The user should provide exact username and password which was given at the time of registration, if login becomes success, it will take up to main page or else it will remain in the login page itself.

SERVICE PROVIDER

- **Resource Provisioning**

Resource provisioning is the process of providing resources to the clients or customers with accounts, the appropriate access to their accounts, all the rights associated with their accounts, and all of the resources required to manage those accounts. When used in reference to a client, provisioning can be thought as a form of customer service.

THIRD PARTY AUDITOR

- **Auditing Process**

In the auditing module, the auditor recognizes the propositions before him that are to be examined, collects the evidence, evaluates the same and on this basis formulates a judgment which is conveyed through his audit report.

DATA OWNER

- **Key Maker**

In the key maker module, keys are generated based on the user setup in order to generate verification Meta data of the uploaded file.

- **Auditing Request**

User can send an auditing request to external auditor along with the signatures and Meta data of the file. After which the auditor will request for the generated proof from the service provider in order to do auditing process. Finally data owner will get the audit report.

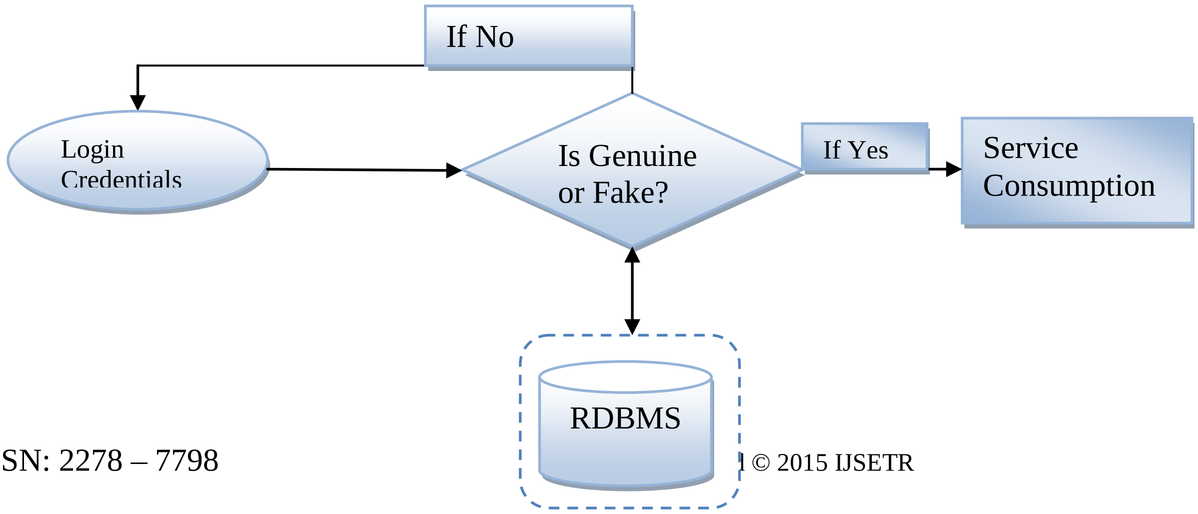
DATA USER

- **Access Cloud Data**

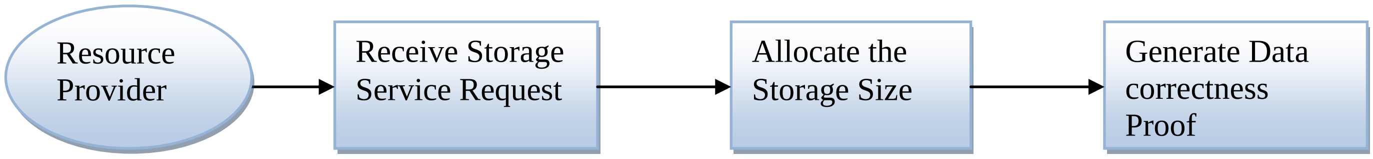
The approved data user will get the keys from the data owner and then access their data from the cloud.

VII. MODULE DIAGRAM

- **Authentication**

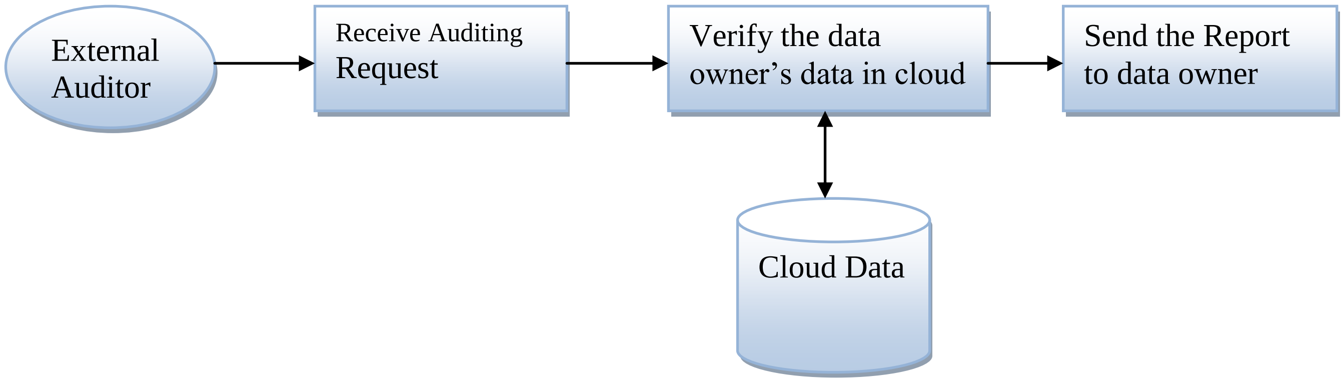


- **SERVICE PROVIDER**
  - **Resource Provisioning**

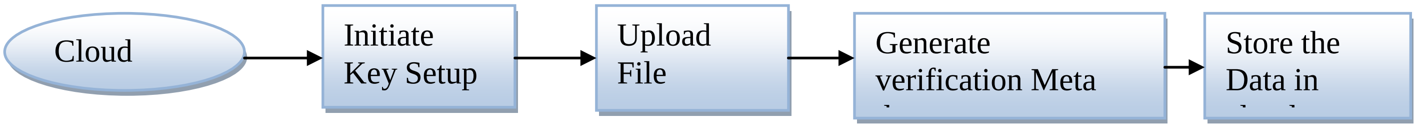

Resource Provider
Receive Storage Service Request
Allocate the Storage Size
Generate Data correctness Proof

THIRD PARTY AUDITOR

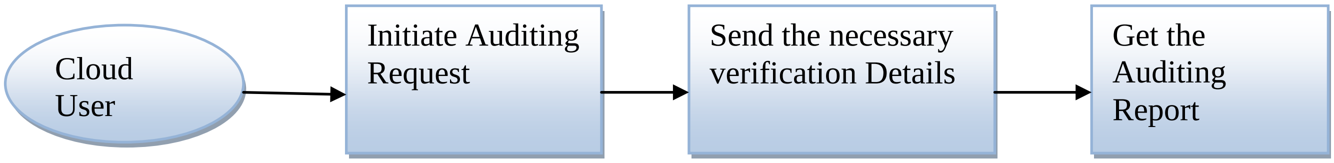
- **Auditing Process**


External Auditor
Receive Auditing Request
Verify the data owner's data in cloud
Send the Report to data owner
Cloud Data

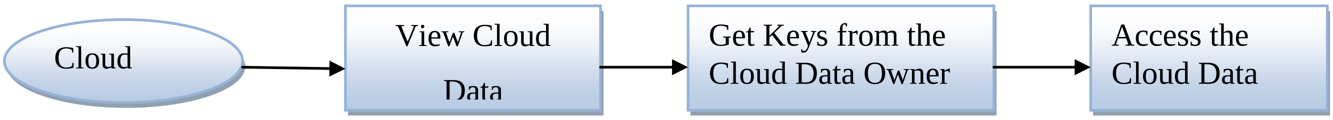
- DATA OWNER
  - **Key Maker**



- **Auditing Request**


Cloud User
Initiate Auditing Request
Send the necessary verification Details
Get the Auditing Report

- **DATA USER**
    - **Access Cloud Data**



Data Flow Diagram :

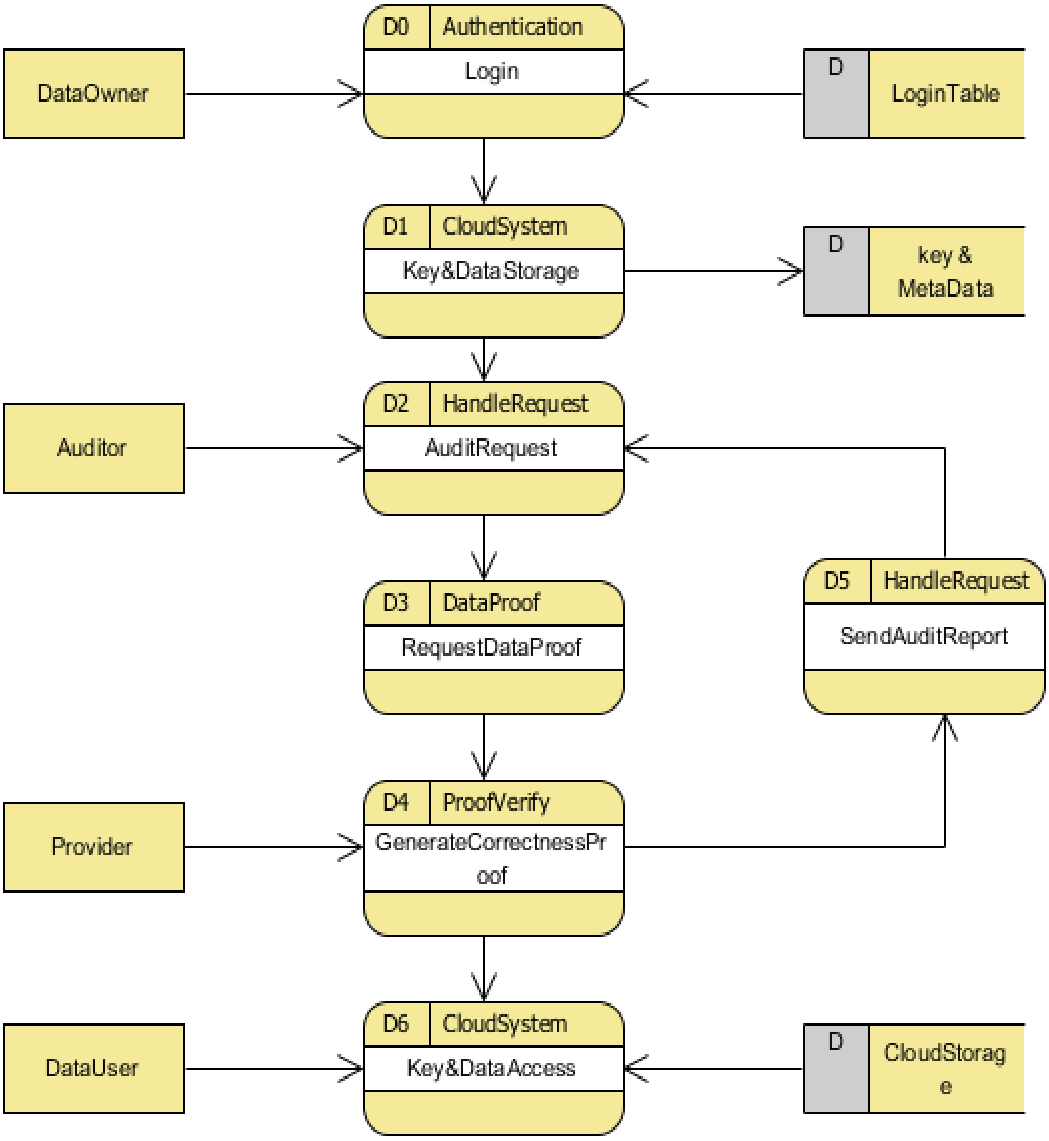


Fig. 1. Data Flow Diagram

VIII. COMPARISON OF VARIOUS SECURITY MECHANISMS IN PUBLIC AUDITING

TITLE	METHOD	ADVANTAGES	DISADVAVTAGES
Scalable and Efficient Provable Data Possession	Secure and Scalable Provable Data Possession scheme	low cost and support for dynamic outsourced data	Not applicable on unreliable servers
Provable Data Possession at Untrusted Stores	Provable Data Possession at untrusted servers	Probabilistic proofs of possession are generated	Data integrity is cannot be checked
Auditing to Keep Online Storage Services Honest	Auditing to check the data integrity	Data stored in the cloud is more reliable and safe	Auditing is an extra burden
Privacy-Preserving Audit and Extraction of Digital Contents	Auditing and Extraction of the stored data	Data stored in the cloud is more reliable and generates copy of the digital contents	Auditing is an extra burden
Toward Publicly Auditable Secure Cloud Data Storage Services	Public Auditing	Copy of data is provided for public Auditing	Public Auditing compromises on Data Privacy
Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing	Introduction of Third Party Auditor	Eliminates the involvement of the client	Data Privacy is compromised

Table 1: Comparison of various security mechanisms in public auditing

IX. CONCLUSION

In this paper, a privacy-preserving public auditing system for data storage security in Cloud Computing is proposed. Homo-Morphic linear authenticator and random masking are utilized to guarantee that the Third Party Auditor would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only removes the burden of cloud user from the tedious and possibly expensive auditing task, but also assuages the users fear of their outsourced data leakage. Considering Third Party Auditing may concurrently handle multiple audit sessions from different users for their outsourced data files. This proposed privacy-preserving public auditing protocol is further extended to a multi-user setting, where a Third Party Auditor can perform multiple auditing tasks in a batch manner for better efficiency. Detailed and Extensive analysis shows that our schemes are provably secure and highly efficient.

X. ACKNOWLEDGEMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, HOD of Computer Science & Engineering, Dr. K.P. Kaliyamurthie, Bharath University,Chennai for their motivation and constant encouragement. The author would like to specially thank **Dr. A. Kumaravel, Dean, School of Computing,** Bharath University for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science &Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, Vol. 22, No. 5, PP. 847-859, May - 2011.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), PP. 598-609, 2007.
3. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
4. C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, Vol. 24, No. 4, PP. 19-24, July/Aug. 2010.
5. M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), PP. 1-6, 2007.
6. R. Curtmola, O. Khan, and R. Burns, "Robust Remote Data Checking," Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS '08), PP. 63-68, 2008.
7. A.L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical Short Signature Batch Verification," Proc. Cryptographers' Track at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA), pp. 309-324, 2009.
8. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), PP. 1-10, 2008.
9. G. Ateniese, S. Kamara, and J. Katz, "Proofs of Storage from Homomorphic Identification Protocols," Proc. 15th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT), PP.. 319-333, 2009.
10. F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures", IEEE Trans. Knowledge and Data Eng., Vol. 20,No. 8, PP. 1034-1038, August - 2008.

[1]**Vaibhav Srikar.M**, Department of C.S.E, Bharath University,Chennai – 600 073, INDIA.

[2]**Ezhil Raj.R**, Department of C.S.E, Bharath University,Chennai – 600 073, INDIA.

[3]**Beema Mehraj.M**, Assistant Professor, Dept. of C.S.E, Bharath University, Chennai, INDIA.