Secured Data Storage with Enhanced Trusted Party Auditing Scheme in Cloud Computing

S.John Justin Thangaraj [1], C.Ashwitha [2], M.Saipriya [3]

[1]AP/CSE, Vel Tech Multi Tech Dr.RR Dr.SR Engineering College. Chennai, India
[2,3]B.E – CSE, Vel Tech Multi Tech Dr.RR Dr.SR Engineering College. Chennai, India
[1] johnjustin@veltechmultitech.org
[2] ashwitha.chandru@gmail.com
[3] saipriya5500@gmail.com

***Abstract*- The correctness of the data in the cloud is being put at risk due to the following reasons, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Therefore, a secure cloud storage system supporting privacy-preserving public auditing. In which the Data owner uploads the data in the Cloud Server and they are allowed to modify the data using the Private Key. The Cloud Sever Stores the data and split those data into the batches using Merkel Hash Tree Algorithm. The TPA will audit the data files that are requested by the Data Owner. The TPA will also audit the multiple files and also implementing the load balancing mechanism to process user requested Job and the Multi Owner authentication mechanism to authenticate the User.**

Keyword- Trusted Party Auditing, Multi Owner Authentication, Cloud Server, Merkel Hash Tree

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application.

A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud . Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues.

Cloud computing takes the technology, services, and applications that are similar to those on the Internet and turns them into a self-service utility. The use of the word “cloud” makes reference to the two essential concepts.

A. Abstraction

Cloud computing abstracts the details of system implementation from users and developers. Applications run on physical systems that aren't specified, data is stored in locations that are unknown, administration of systems is outsourced to others, and access by users is ubiquitous.

B. Virtualization

Cloud computing virtualizes systems by pooling and sharing resources. Systems and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility.

II. RELATED WORKS

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free.

To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

In the existing system, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.

- Security is very low, so that the user is afraid of uploading the data in the Cloud Servers.
- No Proper mechanism was implemented to the audit the data that are stored in the Cloud Servers.
- As Business point of view the customer's of the Company will be reduced by using this poor Data Auditing Mechanism.

III. DESIGN GOALS

To enable privacy-preserving public auditing for cloud data storage under the fore mentioned model, our protocol design should achieve the following security and performance guarantees.

1) Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.

2) Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.

3) Privacy-preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.

4) Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

5) Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

IV. PROPOSED SCHEME

This section presents our public auditing scheme which provides a complete outsourcing solution of data – not only the data itself, but also its integrity checking. After introducing notations and brief preliminaries, we start from an overview of our public auditing system and discuss two straightforward schemes and their demerits. Then we present our main scheme and show how to extent our main scheme to support batch auditing for the TPA upon delegations from multiple users. Finally, we discuss how to generalize our privacy-preserving public auditing scheme and its support of data dynamics.

In the Proposed System, we are implementing the secure system namely Privacy preserving auditing. In this system, first the Data Owner will register with the Cloud Service Providers. During the registration phase the Public and Private will be generated for the Data Owner. The Data Owner have to provide their Private key while updating their data in the Cloud Server. Using Merkle Hash Tree Algorithm the Cloud Server Split the into batches. The Cloud Server will allow the Trusted Party Auditor (TPA) to audit the data that was Stored in the Cloud Server as requested by the User. The TPA will also audit multiple Files also.

We also implement Secure Multi Owner Authentication technique by which we can secure the data Stored in the Cloud Server's Database. First data will be uploaded by the Data Owner in the Cloud Server in the Encrypted format. Also the User wants to View/ Download the data, they have to provide the public key. The Data Owners will check the Public Key entered by the User. If valid, then the decryption key will be provided to the User to encrypt the data. We are also implementing the Load Balancing Concept to Process the User requested Job. First the User request will be past to the Cloud Server and then to the Queues in the Cloud Server. Then the Job will be given to the Virtual Machines presented in the respective Queues.

- By providing the Public and Private key components the user is only allowed to access the data.
- By allowing the Trusted party Auditor to audit the data will increase the Trustworthiness between the User and Cloud Service Providers.
- By using Merkle Hash Tree Algorithm the data will be audited via multiple level of batch auditing Process.
- As Business Point of view, the Company's Customers will be increased due to the Security and Auditing Process.

V. ALGORITHMS AND IMPLEMENTATION

A. MERKLE HASH ALGORITHM

- Data is split into parts.
- Hash function say, H : {0, 1}□ → {0, 1}s is applied.
- Key generation,
- Yij = H(Xij), where i ranges between $1 \leq i \leq k$ and j={0,1}
- 2*k values Yij are public key ,
- Xij values are private key.

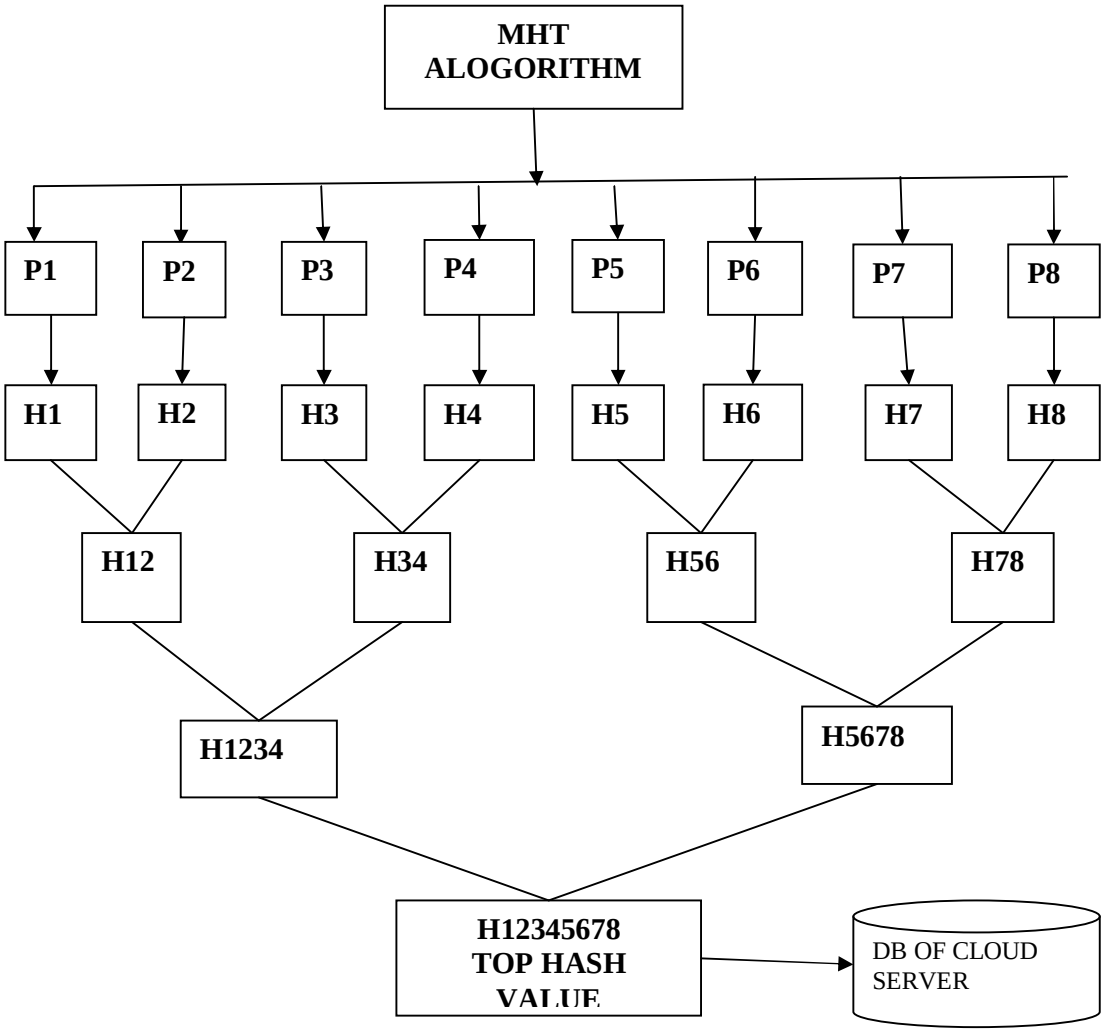

Fig.2 Merkel Hash Tree Algorithm

B. TREE HASH ALGORITHM

Algorithm: TREEHASH (start, maxheight)

1. Set leaf = start and create empty stack.

2. Consolidate: If top 2 nodes on the stack are equal height:

• Pop node value P(nright) from stack.

• Pop node value P(nleft) from stack.

Compute P(nparent) = f(P(nleft||P(nright)).

• If height of P(nparent) = maxheight, output P(nparent).

- Push P(nparent) onto the stack.

3. New Leaf: Otherwise:

- Compute P(nl) = LEAFCALC(leaf).
- Push P(nl) onto the stack.
- Increment leaf.

4. Loop to step 2.

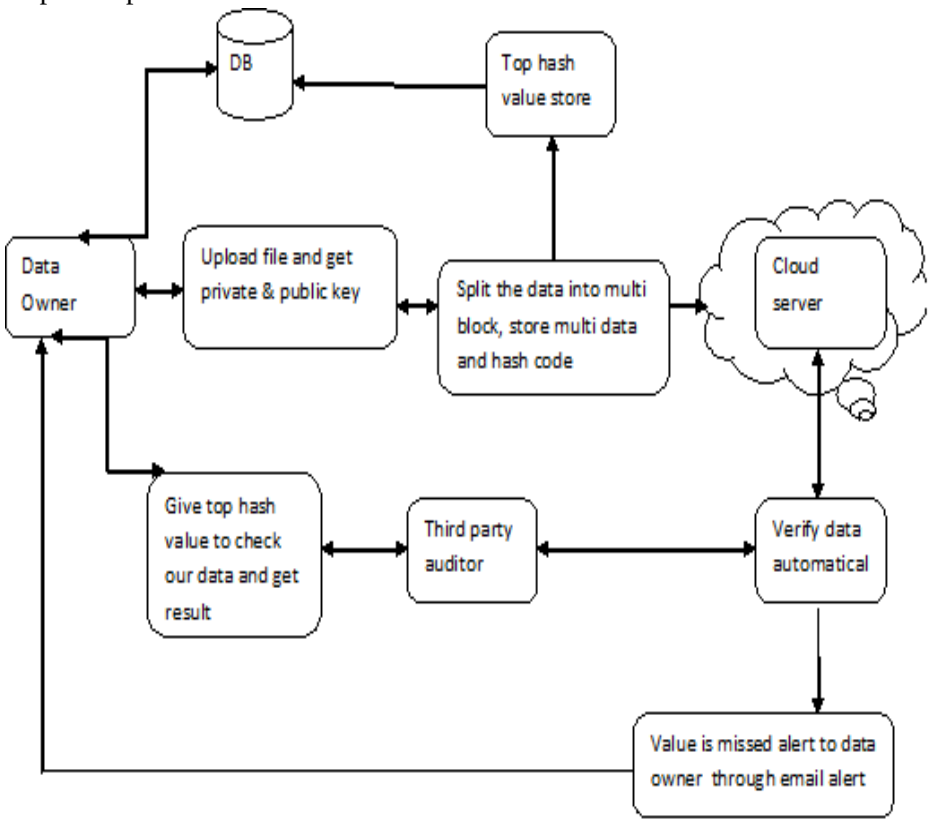

Fig.1 Architecture Diagram

VI. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. We utilize the homo-morphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

ACKNOWLEDGMENT

We wish to express our sincere and gratitude to the HOD of Computer Science & Engineering Mr. R. KARTHIKEYAN, who has been guiding force and constant source of inspiration to us.

We also thank our Project Coordinator and all the staff members of CSE department for the views and comments on our project.

REFERENCES

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

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

AUTHOR PROFILE

S.John Justin Thangaraj Received the M.Tech., Degree in Information Technology from Manonmaniam Sundaranar University, Tamilnadu, India in 2007 and B.E., Degree in Computer Science & Engineering in Government College of Engineering, Tirunelveli, affiliated to Manonmaniam Sundaranar University, Tamilnadu, India in 2001. He is presently working as Assistant Professor in CSE, at Vel Tech Multi Tech Dr.RR Dr.SR Engineering College, Chennai. His Current area of research is Wireless Network.

C.Ashwitha & M.Saipriya Doing B.E., Degree in Computer Science & Engineering in Vel Tech Multi Tech Dr.RR Dr.SR Engineering College, Chennai, affiliated to Anna University, Tamilnadu, India.