Indian Journal of Research in Applied Sciences Engineering (IJRASE)
Vol.2.No.1 2014pp 44-46.
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

SECURED DATA STORAGE WITH ENHANCED TPA AUDITING SCHEME USING MERKLE HASH TREE IN CLOUD COMPUTING

Mr.E.Ezhilarasan [1]and Mrs .Thamaraiselvi [2]
Department of Computer Science and Engineering, SCSVMV University Enathur
Ezhilmarch12@gmail.com[1]

ABSTRACT

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. 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 also. We are implementing the load balancing mechanism to process user requested Job and also implementing the Multi Owner authentication mechanism to authenticate the User.

Keywords: cloud storage, privacy-preserving, public auditing, Merkel Hash Tree Algorithm, TPA(Trusted part auditor).

1. INTRODUCTION

. CLOUD COMPUTING

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:

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.

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 **.**

1.2 SYSTEM OVERVIEW

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.

2.1EXISTING SYSTEM:

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.

Disadvantges:

Security is very low ,so that the user are 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.

2.2 PROPOSED SYSTEM:

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.

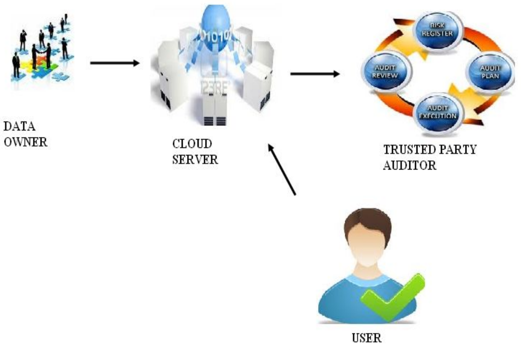
2.3 MODIFICATION:

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 Queue 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.

2.2 System Architecture:

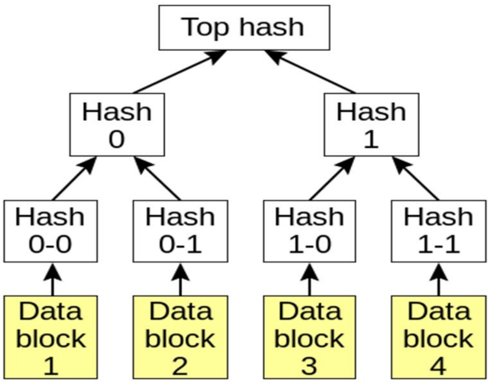


2.2.1 System Architecture

3. Algorithm:

3.1Merkle hash tree algorithm:

Once the data owner send the request to audit the data that will be audited by the Trusted Party auditor using Merkle Hash tree Algorithm. The data will audited by dividing the data into multiple parts. After each time Period, the auditing information will be updated by the Trusted Party Auditor. So that we can ensure security. If there is any change while auditing the data, the TPA will address the same to the Data Owner.



3.1.1Merkle hash tree algorithm

3.2AES algorithm:

Four different stages are used,

1.Substitute bytes: uses an S-box to perform a byte by byte substitution of the block.

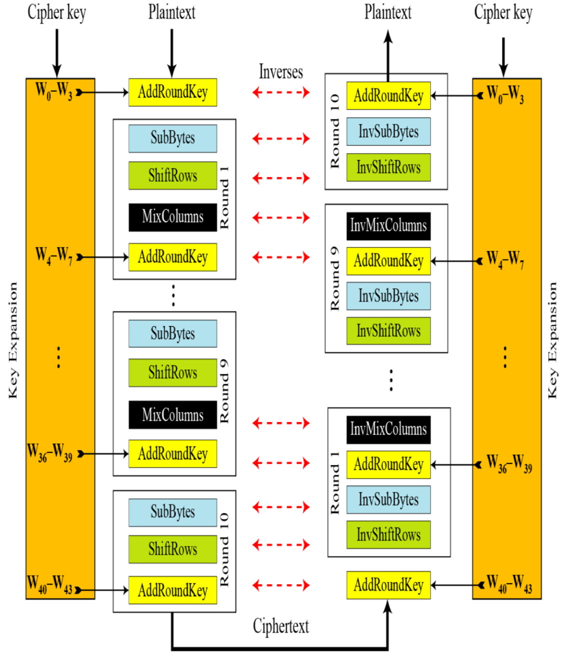
2.Shift Rows: A simple permutation.

3.Mix columns: A substitution that makes use of over 128 bits.

4.Addroundkey: A simple bitwise XOR of the current block with a portion of the expanded key.

Both encryption and decryption the cipher begins with an

AddRound key stage.



4.CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. We utilize the homomorphic 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. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently.

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.

[1]. G. Miller, C. Fellbaum, R. Tengi, P. Wakefield, and H. Langone, "Wordnet Lexical Database," http://wordnet.princeton.edu/wordnet/download/ , 2009.

[2]. http://extjwnl.sourceforge.net/
P. Resnik, "Semantic Similarity in a Taxonomy: An Information- Based Measure and Its Application to Problems of Ambiguity in Natural Language," J. Artificial Intelligence Research, vol. 11, pp. 95- 130, 1999.