International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Special Issue 01 | 2020

Merkle Hash Tree based Integrity Framework with Secure Auditing

[1]Mr. Khandare Pramod P., [2]Mr. Shekh Shahrukh I.

[1]*Principal, SIET (Poly), Paniv (India)*
[2]*Head of Computer Department, SIET (Poly), Paniv (India)*

ABSTRACT

Main call for Cloud computing is that users only utilize what they required and only pay for whatever they are using. Cloud Computing refers to an infrastructure where data processing and storage can happen away from device. The storage of data on cloud there is an issue of data security. So there is risk associated with data storage many IT professionals are not showing their interest towards Cloud Computing. To ensure the user"s data correctness in the cloud storage proposing an effective mechanism with salient feature of data integrity and authentication. (Third Party Auditing) TPA checks the integrity of the data stored on mobile cloud without of the data owner. TPA checks the hash value and message to verify the integrity of the data. The Integrity Verification is provided by the TPA which minimizes much more work of the user. In proposed system data owner has chosen two keys, one of which is only known to him called private key and another is public key.

So this provides the confidentiality to the data of mobile user. Hence the system proposed system emerge a solution which uses the DES algorithm for data integrity and mechanism of hash function along with Merkle Hash Tree encryption tool to provide better security to the authentic data stored on the cloud. The model of cloud not only solve the problem of storage of authentic data, but also make sure that it will give data access control mechanisms and ensure sharing data. In the proposed scheme a proof of data integrity is preserved with data authentication and data integrity verification.

Keywords : Cloud; confidentiality; Data security; Merkle Hash Tree.

1. INTRODUCTION

The cloud computing has converted popularity in recent technological fields. Cloud computing is merging of multiple existing technologies such as web computing, parallel and distributed computing, grid computing, utility computing, virtualization etc. Cloud is highly special as when it comes to huge data storage and can provide computing resources on demand. The aim of cloud security is to provide a practical reference to access information technology (IT) and business decision makers as they ensure and preserve the security implications of cloud computing on their business.

Cloud storage provides customers with benefits, ranging from cost saving and simplified convenience, to mobility opportunities and scalable service. These great features attract more and more customers to utilize the storage of their personal data to the cloud storage. The cloud servers mostly utilized to relieve clients from the intensity of storage management and maintenance. The mostly difference of cloud storage from traditional in-house storage is that the data is parsed via Internet and stored in an uncertain domain, which inevitably raises clients great concerns on the integrity and authentication of their data.

Cloud computing security, performance and availability are having three hot spots of the cloud computing research. The top of research is cloud computing security. Based on the three special different definitions of cloud computing such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), cloud computing can be divided into three levels: the infrastructure layer, platform services layer, application layer software. To the highest level of SaaS, the problems of data and application security are gained more attention. Furthermore, when SaaS is constructed on the platform of the cloud computing, most of these security issues on the highest layer are unknown and uncontrollable. [1]

2. LITERATURE REVIEW

Cloud storage has providing a solution that convenient and on-demand accesses to large amounts of data spread over the Internet. Today, number of users wants to share personal data, like photos and videos, with their friends through the social network applications [1]. Cloud storage has become popular by business users due to its vigorous benefits, proceeding lower cost and better resource utilization. Nowadays users connected to the Internet may store their data on cloud servers and the cloud servers manage or process their data for respective applications [2].

The current Cloud security model is based on the assumption that the user/customer should trust the provider. This is typically governed by a Service Level Agreement (SLA) that in general defines mutual provider and user expectations and obligations [4]. In order to ensure the integrity and availability of data in

Cloud and enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. However, the fact those users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional authentic primitives for the purpose of data integrity protection using MHT algorithm [3].

2.1 Merkle Hash Tree

The binary tree each node having two child nodes, according to this algorithm every non leaf node having two child nodes. Information enclosed in one node N in an MHT T is constructed as follows. For a leaf node based on a file block m_i, node value is computed as $h_i = H(m_i)$. A parent node of N_1 and N_2 is constructed as $N_P = \{H(h1_{||}h_2)\}$.

2.2 Ranked Merkle Hash Tree (RMHT):

A Merkle Hash Tree is a narrative authenticated data structure designed for proficient verification of data updates by ranks, known as RMHT. Cloud is extremely scalable when it comes to enormous data storage; the *Cloud Service Providers (CSP)* use common strategies to improve data reliability and availability such as storing multiple replicas beside with original datasets by public data auditing scheme to verify outsourced data storage exclusive of having to retrieve the overall datasets that why MHT system overcome the lacuna using data dynamics and the public auditing schemes.

The proposed system proves the authentication and integrity with improving the data auditing and replication for cloud data storage. Users are firstly uploading the data with delegation means that cover required or initiated data. The security and authentication system uses the MHT based algorithm that improves the efficiency, bandwidth in terms effectiveness of cloud data.

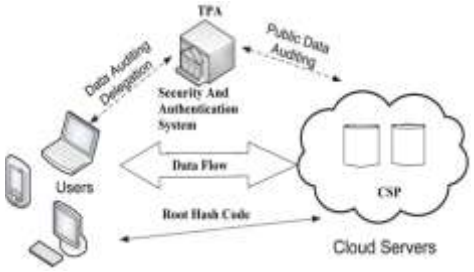

Fig 1: System Architecture

3. SYSTEM ARCHITECTURE

There are several aspects which purpose specified by the Merkle tree traversal algorithms for cloud secures storage. These are the hash function, the deterministic pseudo–random number generator and the algorithm worn for the leaf calculation. The concluding is defined by the usage of the tree and structure of tree depends on node. The hash function used for the traversal algorithm must be avoiding the collision. Thus the main assortment criteria for the hash function are good performance and strong security.

In cloud computing public auditing ability and data dynamics for remote data integrity are checked. The system construction is conceptually designed to compute these two important goals while efficiency being also measured. To achieve efficient data dynamics, the system improves the existing proofs of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication and integrity.

- The Third Party Auditor (TPA) is trusted who does not generate any security troubles.
- There might be dormant storage inconsistencies that are not disclosed through cloud service providers.
- Cloud service providers may remove some data of data owner for economic gains or other reason.

3.1 Setup Phase

The setup algorithm initial algorithm for proposed module. So that takes no input firstly and outputs the root hash code for the input. For a leaf node based on a file block m_i, node hash value is computed as $h_i = H(m_i)$.

3.2 Encryption Phase

Encrypt (spk, M, J). The encryption algorithm fetches as input the public parameters sp_K, a message M, and a right of entry structure J over the universe of attributes. The algorithm will encrypt M and construct a cipher text CT such that only a user that possesses a set of attributes that satisfies the access structure will achieve decryption the message.

3.3 Keygen Phase

The client generates a secret value $\alpha \in Z_p$ and a generator g of G, then compute $v=g^{\alpha}$. A secret signing key pair {*spk, ssk*} is chosen with respect to a designated provably secure signature scheme whose signing algorithm is denoted as Sig(). This algorithm outputs {*ssk, α*} as the secret key *sk* and {*spk, v, g*} as the public key *pk*. For simplicity, in our settings, we use the same key pair for signatures, i.e., *ssk=α, spk* = {*v, g*}.

3.4 Decrypt Phase

Decrypt (spk, CT, ssk). The decryption algorithm takes as input the public parameters spk, a cipher text CT, which contains an access policy J, and a private key ssk, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure J then the algorithm will decrypt the cipher text and return a message M.

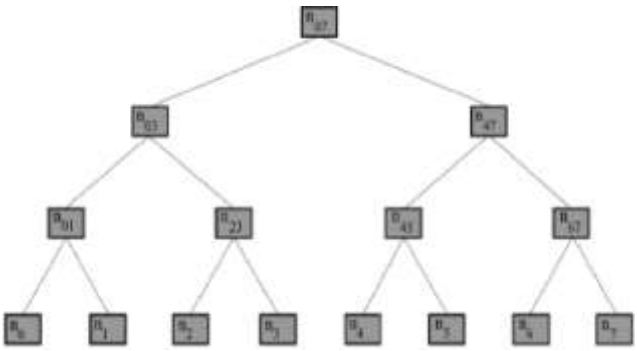

Fig 2: Merkle tree with 8 leaves. The root can be used to authenticate the complete tree.

4. SYSTEM MODULES

4.1 Data Owner

In this module we are going to create a User application by which the data owner is allowed to access the application provided by the cloud. First the data owner registers his details with the Cloud Service Provider. Once registered the private key generated will be send to the Data owner mail id given at the time of registration. The registered Data owner is allowed to upload the files into the Cloud Sever. The file will be encrypted using Advanced Encryption Scheme and then upload into the Cloud Server.

4.2 Merkle Hash Tree

Merkle Hash Tree is tree in which every non-leaf node is labeled with the hash of labels of its children node. MHT is based on binary tree which is useful because they allow efficient and secure verification of the contents of data structures. Those encrypted form of data would be split into batches and those batch files are stored in cloud. In the root node top hash key stored in local database of data owner. In this algorithm given an authentication path and a leaf, one can verify the correctness of the latter with respect to the publicly known root value.

4.3 Cloud Service Provider

Cloud Service Provider (CSP) contains the large amount of data in their Data Storage. Also CSP will maintain all the User information to authenticate when they want to login into their account. Also the Cloud Server will redirect the User requested job to any of the Queue to process the User requested job. The request of all Users will be processed by the Virtual machines in the Queue.

5. PERFORMANCE EVALUATIONS

The system which able to occupy some extraordinary things for technical importance can be measured with parameters. So survey of the paper mostly prepared with problem statement and that helps for performance measurement of system. Initially the public auditability should prove the existence of novel scheme of Merkle Hash Tree algorithm. Especially the new fact of system emerged on the one iteration for updating all replicas at once. Hence it helps for emerge the time and the space complexity with bandwidth specification.

Table 1: System analysis with parameters

	MR- PDP [2]	SiR –PA [3]	FU- DPA [4]	Proposed Scheme
Public Auditability	**No**	**Yes**	**No**	**Yes**
Authorized Auditing	No	No	Yes	Yes
One Interaction for Updating All Replicas	**No**	**No**	**No**	**Yes**

In system provided investigational results has to accomplish the improved efficiency of MuR-DPA when deployed on cloud data storage. We evaluate our new scheme, MuR-DPA MR-PDP, DPDP, SIR-DPA, schemes and our proposed system is once who providing the system public auditing and all replica updating with single iteration.

The proposed system provides structure with salesfoce cloud testing with measure superior performance. Cloud storage behavior and the time cost for auditing the file has occupied superior confidence.

6. ACKNOWLEDGMENTS

This research was supported by Principal Mr. Khandare P.P working as principal of SIET (Poly), Paniv institute also Hon Mr. Shahrukh Shekh as Head of Department. We thank our colleagues from Shriram Institute of Engineering and Technology (Poly), Paniv who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper. We thank Ms. Rajani Sajjan working on cloud data security and appearing PhD of Computer Science for assistance with Cloud Data Security, and Ms. Ekatpure S.A. as senior lecturer of SIET (Poly), Paniv for comments that greatly improved the manuscript.

7. REFERENCES

[1] Rajani Sajjan "Cloud Security and Authentication using MHT", Springer International Publishing AG 2018 P.M. Pawar et al. (eds.), Techno-Societal 2016, DOI 10.1007/978- 3-319-53556-2_108.

[2] R. Curtmola, O. Khan, R. C. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th IEEE Int.Conf. Distrib. Comput. Syst., Beijing, China, 2008, pp. 411–420.

[3] C. Erway, A., C. Papamanthou, and R. Tamassia, "Dynamic provable data possession", in Proc. 16th ACM Conf.Comput.Commun. Security, Chicago, USA, 2009, pp. 213–222.

[4] 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 Distrib. Syst., vol. 22, no. 5,pp. 847–859, May 2011.

[5] C. Liu, J. Chen, L. T. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanarao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," IEEE Trans. Parallel Distrib. Syst., 2014.

[6] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, Senior Member " MuR-DPA: Top-Down Levelled Multi-Replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud " IEEE Transactions On Computers, Vol. 64, No. 9, September 2015

[7] Yubin Xia, Yutao Liu, Haibing Guan, Yunji Chen, Tianshi Chen, Binyu Zang, Haibo Chen, "Secure Outsourcing of Virtual Appliance" IEEE Transactions on Cloud Computing DOI. 2015

[8] Christina Delimitrou and Christos Kozyrakis Security Implications of Data Mining in Cloud Scheduling", IEEE Computer Architecture Letters 2015

[9] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, „„Cooperative Provable Data Possession for Integrity Verification in Multi- Cloud Storage"", IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[10] X. Zhang, C. Liu, S. Nepal, S. Panley, and J. Chen, „„A Privacy Leakage Upper-Bound Constraint Based Approach for Cost- Effective Privacy Preserving of Intermediate Datasets in Cloud,"" IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1192-1202, June 2013.

[11] Jin Li, Xiaofeng Chen, Xinyi Huang, Shaohua Tang and Yang Xiang *Senior Member, IEEE* and Mohammad Mehedi Hassan *Member, IEEE* and Abdulhameed Alelaiwi *Member, IEEE* "Secure Distributed Deduplication Systems with Improved Reliability" IEEE Transactions on Computers. 2015