Secure Signature Generation for Dynamic Audit Services in Cloud Data Storage

[1]Madasu Kalpana, [2]Vakamalla Siva Sankar Reddy
[1,2]Dept. of CSE, QIS Institute of Technology, Ongole, AP, India

Abstract

Maintaining data determined quality in public cloud acts an essential measure in cloud computing. Cloud storage auditing settles the multifaceted nature of data dependability in public cloud. In advance auditing protocols are all standard on the announcement that the customer's private key for auditing is totally secured. Nonetheless, such proclamation most likely won't for untouched be seized, in light of the presumably weak rationale of insurance or potentially low security settings at the customer. In the event that such a mystery key for auditing is revealed, almost every one of the current auditing protocols would unquestionably form into unable toward effort. In this paper, we meeting point happening this new part of cloud storage auditing. We analyze how to diminish harm of the customer's key scope in cloud storage auditing, and give the essential sensible answer for this unique trouble setting. We commend the significance and the shelter model of auditing convention with key-scope adaptability and propose such a convention. In our arrangement, we use the preorder traversal method and the twofold tree structure to illuminate the private keys for the buyer. Not with standing grow a novel authenticator structure to maintain the forward security and the advantages of lump less obviousness. The asylum verification and the presentation examination demonstrate that our proposed convention is sheltered and capable.

Keywords

Data Storage, Cloud Storage Auditing, Cloud Computation, Key-Exposure Resistance.

I. Introduction

Cloud Computing is a worldview where massive pool of frameworks are associated in private or public systems to give progressively adaptable foundation to application, data and file storage. The outsourced storage in clouds has turned into another benefit development point by giving a tantamount ease, versatile, area autonomous stage for dealing with customer's data. The cloud storage eases the weight for storage administration and upkeep. It moves the application programming and databases to the brought together extensive server farms, where the administration of the data and administrations may not be completely reliable. One of the greatest worries with cloud data storage is that of data honesty confirmation at untrusted servers. Security review is a critical arrangement empowering follow back and examination of any exercises including data get to, security breaks, application exercises et cetera. Outsider examiner is an acknowledged strategy for foundation trust between two gatherings with conceivably unique motivations [2]. Examiners survey and uncover chance, empowering clients to pick reasonably between contending administrations. We think auditing is vital for conventional business as well as for online administrations. One approach to depend on a trusted outsider reviewer, who has adequate access to the supplier's surroundings. An examiner comprehends the administration level assention (SLA) between a client and a supplier and measures the degree to which the supplier won't not meet the SLA. We recognize auditing by two methodologies outside and inside auditing. Considering the part of verifier in the model, every one of the plans displayed before fall into two classifications: private and public auditability [2]. Although plans with private auditability can accomplish higher plan proficiency, public auditability permits anybody not only the customer to challenge The cloud server for rightness of data storage while keeping no private data. At that point, customers can assign the data of the administration execution to the free outsider examiner without commitment of their computational assets. Another significant worry among past outlines is that of supporting element data operation for cloud data storage applications. In Cloud Computing, the remotely put away electronic data may be gotten to as well as upgraded by the customers, e.g., through piece alteration, erasure and inclusion, and so forth. Lamentably, the condition of the - craftsmanship with regards to remote data storage mostly concentrate on static data documents and the significance of this Dynamic data upgrade has gotten constrained consideration so far [1], [7]. In addition, as will be demonstrated later, the immediate augmentation of the current provable data ownership (PDP) [2] or evidence of retrievability (POR) [4] with plans to bolster data elements may prompt to security escape clauses. In spite of the fact that there are numerous challenges confronted by specialists, it is very much trusted that supporting element data operation can be of indispensable significance to the commonsense use of storage outsourcing administrations. In perspective of the key part of public auditability and data elements for cloud data storage, we propose a proficient development for the consistent coordination of these segments in the convention plan. We manage customer's mystery key presentation which is a noteworthy worry to the convention in cloud storage. In past work, protocols outlined didn't consider the issues confronted because of the introduction of key in public cloud. In this paper, we concentrate on the best way to decrease the issues, for example, permitting copy data, security issues, computational time and vitality utilization because of review utilizing remote servers. Past process includes recovering entire data or the data that is known to confirm yet in this outline we make a private security for each client by making bunches in public cloud. Besides, embrace the measures of outsourcing the data without the learning and presentation of key in either public or private cloud. Here, the auditing [10] is guaranteed by blocked confirmation in public cloud.

II. Related Work

With a specific end goal to check the trustworthiness of the data put away in the remote server, numerous protocols were proposed [4] These protocols concentrated on different prerequisites, for example, high proficiency, stateless confirmation, data dynamic operation, security insurance, and so on. As indicated by the part of the evaluator, these auditing protocols can be partitioned into two classes: private check and public confirmation. In an auditing convention with private unquestionable status, the inspector is furnished with a mystery that is not known to the demonstrated or different gatherings. Just the examiner can confirm the honesty of the data. Conversely, the check calculation does not require a mystery key from the evaluator in an auditing convention with public unquestionable status. Along these lines, any outsider can assume the part of the inspector in this sort of auditing protocols. Ateniese et al. [1] firstly considered the public check and proposed the thought of ―Provable Data Possession‖ (PDP) for guaranteeing data ownership at untrusted storages. They utilized the procedure of HLA and irregular example to review outsourced data. Juels and KaliskiJr. investigated a ―proof of retrievability‖ (PoR) show. They utilized the apparatuses of spot-checking and errorcorrecting codes to guarantee both ownership and retrievability of documents on remote storage frameworks. Shacham and Waters [6] gave two short and productive holomorphic authenticators: one has private obviousness which depends on pseudorandom works; alternate has public undeniable nature which depends on the BLS signature. Dodis et al. [3] concentrated on the review on various variations of existing POR work. Shah et al. acquainted a TPA with keep online storage genuine. The convention requires the reviewer to keep up the state, and experiences limited use. Wang et al. [5] gave a public auditing convention that has protection saving property. Keeping in mind the end goal to make the convention accomplish security saving property, they coordinate the HLA with arbitrary covering system. Wang proposed an intermediary provable data ownership convention. In this convention, the customer appoints its data honesty checking errand to an intermediary. Dynamic data operations for review administrations are likewise gone to keeping in mind the end goal to make auditing more adaptable. Ateniese et al. [2] firstly proposed an incompletely dynamic PDP convention. Wang et al. [7] proposed another auditing convention supporting data progression. In this convention, they used the BLS-based HLA and Merkle Hash Tree to bolster completely data elements. Erway et al. [8] augmented the PDP display and proposed a skip listbased convention with flow bolster. Zhu et al. proposed an agreeable provable data ownership convention which can be reached out to bolster the element auditing. Yang and Jia [9] proposed an element auditing convention with protection safeguarding property. The issue of client repudiation in cloud storage auditing was considered in [10]. The majority of above auditing protocols are altogether based on the supposition that the mystery key of the customer is completely secure and would not be uncovered. Be that as it may, as we have demonstrated beforehand, this suspicion may not generally be valid. The present work progresses the field by investigating how to accomplish key-introduction resistance in cloud storage auditing, under the new issue settings.

III. Problem Statement

The system model consists of three participating entities: data user, CSS and TPA. In fig. 1, we present a sketch of cloud storage architecture and interactions among involved entities. The CSS is server hosted in cloud and supervised by CSP to provide online storage services. The DO possesses massive data that are to be stored on CSS. A third party TPA, who has expertise and capability to do auditing task, is delegated by DO to check data integrity on behalf of DO. TPA periodically audits outsourced data on CSS and informs DO results. Fig. 1. Architecture of Cloud Storage Service and Interactions among Entities Due to public auditability, any entity can obtain public parameters, like public keys, and challenge CSS for data integrity proof. If a malicious entity controls masses of computers that needn't have much computing capability, then it can produce a challenge request flood to CSS in a short time and cause service degradation of CSS, i.e. DDOS attack. However, preserving high quality of service is critical for online service, since the long response latency or even being out of service is terrible for user which may result in the user financial loss. To protect CSS from DDOS attack, C. Liu et al. [13] proposed that DO delegates TPA for data verification with an authorization. When TPA conducts an auditing, it needs to present the authorization in challenge request to CSS for validation. Only when the authorization is valid will CSS generate proof to reply the request. However, CSS can still be affected by DDOS under this solution. Since TPA may be intruded by crackers, performed improper operations by managers or bribed by malicious entity, the authorization of TPA is thus revealed. Once malicious entities obtain authorization, they can make valid challenges with no limitation again. In our construction, auditing number is proposed and integrated into authorization. Auditing number is the maximum challenge times that TPA can make for one data file, which is determined by DO and TPA. It is a practical scenario that DO pays TPA for auditing service and decides how many audit times according to the charging metric of TPA. On cloud side, the current audited number that how many challenges have been issued is recorded. When TPA makes a valid challenge, CSS will increase the current audited number. Once the current audited number reaches constrained auditing number, CSS will reject the challenge requests ever after.

IV. Third Party Auditor

The audit in cloud computing is broadly classified into three, they are first party auditor or internal auditor where the cloud user organization audits by its own, it is a self-assessment procedure for intrusion detection and prevention system. Second party auditor is a Cloud Service Provider who has significant resources and experts in building and managing distributed cloud storage servers, owns and operates where an external auditing procedure is used for data security and quality management in cloud services. The Cloud data storage architecture consists of three actors, the cloud user who has large amount of data to be stored and retrieved as per the requirement in the cloud. The cloud service provider who maintains the cloud storage services and provides cloud data storage. To enable privacy preserving public auditing for cloud data storage shown in the model, the protocol we designed should achieve the following prevention, protection and performance guarantees;

1. **Storage Accuracy:** To ensure that the users data are indeed stored appropriately and kept all the time in cloud.
2. **Reliable Security:** To ensure that the TPA cannot gain users data from the information collected during the auditing process.
3. **Group auditing:** To enable TPA provide secure and efficient auditing to possible large number of different users simultaneously
4. **Detection and Prevention:** To allow TPA to provide auditing with minimum communication.

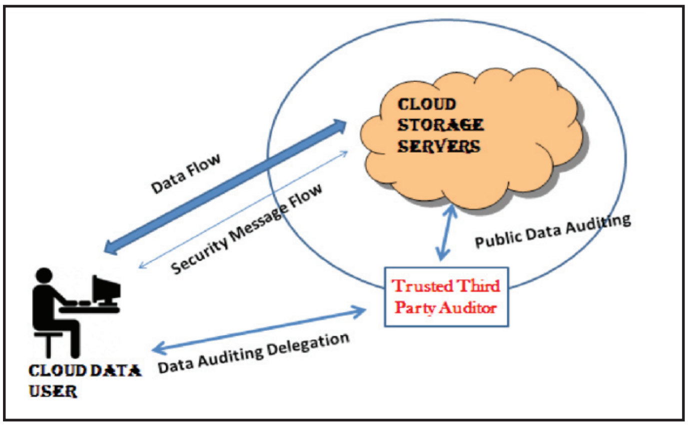

Fig. 1: The Architecture of Cloud Data Storage Services

The Trusted Third Party (TTP) is an audit based organization which facilitates secure interactions between two parties that is cloud user and cloud provider, where both of them trust this third party. The Third Party Auditor (TPA) registered security service provider allocated by the cloud service provider with strong Authentication and Authorization. The TPA can perform Multiple Auditing Tasks for single or multiple clouds in branch manner for better efficiency and security [6]. Public audit-ability: 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.

V. System Model

A. Cloud Server

A local Cloud which provides priced abundant storage services are been created in this module. The users can upload their data in the cloud. This module can be developed where the cloud storage can be made secure. The cloud is not fully honorable by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to that the cloud server is genuine but curious. That is, the cloud server will not maliciously delete or modify user data due to the protection of data investigating schemes, but will try to learn the content of the stored data and the identities of cloud users. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which are supposed to presumably for a fee truly store the data with it and provide it back to the owner whenever required.

The cloud server provides privilege to generate secure multi-owner data sharing scheme called MONA. It denotes that any user in the group can securely share data with others by the cloud. This scheme is able to support dynamic groups comfortably. Respectively, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners but within the group.

Proxy Server Deployment

Group manager takes charge of followings,

1. Signature Generation

- Signature Verification
- Content Regeneration

A proxy agent acts on behalf of the data owner to regenerate authenticators and data blocks on the servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may become off-line after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy. Considering that the data owner cannot always stay online in practice, in order to other group content he will be revoked by the cloud server.

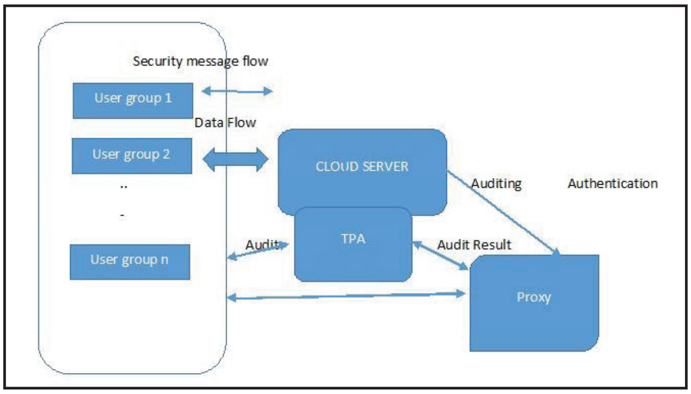

Fig. 2: Cloud Regeneration Architecture

VI. Proposed System Architecture

This paper involves three parties: the cloud server, the Third Party Auditor (TPA) and users is shown in Figure 3. There are two types of users in a group: the original user and a number of group users. The original user and group users are both members of the group. Group members are allowed to access and modify shared data created by the original user based on access control polices. Shared data and its verification information (i.e. Mac code) are both stored in the cloud server. The third party auditor is able to verify the integrity of shared data in the cloud server on behalf of group members.

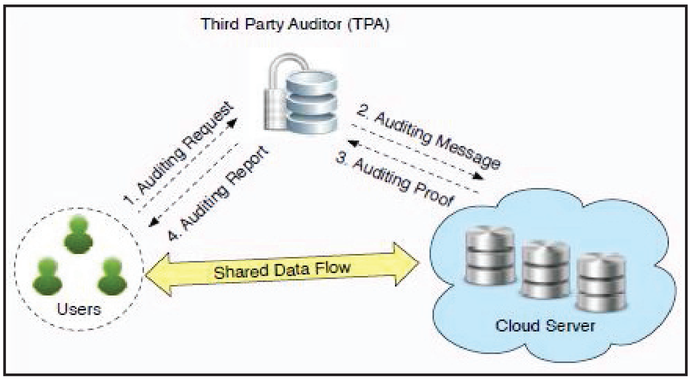

Fig. 3: System Model Includes User, Cloud Server and TPA

In this paper, we only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing. The original user is responsible for deciding who is able to share her data before outsourcing data to the cloud. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing request, the TPA generates an auditing message to the cloud server, and retrieves an auditing proof of shared data from the cloud server. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

A. Proposed Algorithm

Authentication, Authorization and Auditing for secure cloud storage is implemented on the basis of the following key points

1. Our System Supports an External auditor to audit users outsourced data in the cloud without learning knowledge on the data content.
2. The TPA supports scalable on request by cloud service provider for efficient public auditing in the cloud computing
3. Auditing is the processes which is done for the cloud to achieve batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA
4. The auditing is the intelligence based Dynamic data process for the data and information security in cloud computing
5. data integrity algorithm such as Message Authentication Code (MAC code) by means of Hash Based Message Authentication Code (HMAC code) to check the integrity of the data being stored in the cloud.
6. By means of MAC code, we enhance the data integrity of the cloud data.

Step 1: Start of an Algorithm
Step 2: Key Generation by Advanced Encryption Standard (AES) Algorithm 16-bit Hexa Decimal keys are generated
Step 3: Map the Key to the files
Step 4: Divide the files into the blocks
Step 5: Each Encrypted Block is Associated with Key
Step 6: Store the data blocks to the Cloud Storage Server
Step 7: Simultaneously Intelligent system sends a copy of keys to TPA
Step 8: On request of Cloud Service Provider (CSP) the Auditing processes with be done by TPA
Step 9: Validate the data by signatures and data integrity proofs
Step 10: Successful validation, verification will be done for dynamic auditing by TPA End of Algorithm.

VII. Conclusion

Conclusion and Future Work In this paper, we study on how to deal with the client's key without exposing into the cloud. The auditing performed by public verifier not only audits the data but also verifies the integrity of the data in cloud. The concept of user revocation allows to revoke the invalid key registered. We formalize the definition and the security model of auditing protocol without key-exposure resilience, and then propose and verify the first practical solution. Further the duplicated files are prohibited but do not address the issues due to creation of such files. In future we need to identify the solution for providing privacy to data that is not verified in public cloud

References

[1] Jia Yu, KuiRen, Cong Wang, Vijay Varadharajan, "Enabling Cloud Storage Auditing with Key-Exposure Resistance", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 6, June 2015.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song,"Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.

[3] G. Ateniese, R.D. Pietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. 4th International Conference on Security and Privacy in Communication Networks, 2008.

[4] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, J. Quisquater,"Efficient Remote Data Integrity checking in Critical Information Infrastructures," IEEE Transactions on Knowledge and Data Engineering, Vol. 20, No. 8, pp. 1-6, 2008.

[5] R. Curtmola, O. Khan, R. Burns, G. Ateniese,"MRPPDP: Multiple-Replica Provable Data Possession," Proc. 28th IEEE International Conference on Distributed Computing Systems, pp. 411-420, 2008.

[6] H. Shacham, B. Waters,"Compact Proofs of Retrievability," Advances in Cryptology-Asiacrypt'08, pp. 90-107, 2008.

[7] C. Wang, K. Ren, W. Lou, J. Li,"Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, Vol. 24, No. 4, pp. 19-24, July/Aug. 2010.

[8] Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conference on Computer and Communications Security, pp. 756-758, 2010.

[9] K. Yang, X. Jia,"Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," World Wide Web, Vol. 15, No. 4, pp. 409-428, 2012.

[10] K. Yang, X. Jia,"An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Trans. Parallel and Distributed Systems, Vol. 24, No. 9, pp. 1717-1726, 2013.