A SURVEY ON SECURE SHARING AND AUDITING PROCESS USING PRIVACY PRESERVING TOOL IN CLOUD DATA STORAGE

HariPrakash¹, J.Pradeep², E.Kodhai³, Dr. Md. Ali Hussain⁴, Dr. V. RamaKrishna⁵
¹,³Dept of CSE, ²Dept of ECE, SMVEC, Pondicherry, India
⁴Department of ECE, KL University, Green Fields, Vaddeswaram, India.
⁵Department of CSE, KL University, Green Fields, Vaddeswaram, India.
{hariuthirapathi, pradeepece2003, kodhaiej}@gmail.com, dralihussain@kluniversity.in, ramakrishna@kluniversity.in

Abstract: The advent of the cloud computing makes storage outsourcing becomes a rising trend that promotes the secure remote data auditing a hot topic that appeared within the analytical literature. Some analysis has contemplated the problem of security and economical public information integrity auditing for shared dynamic information. However, these schemes are a unit still not secure against the collusion of cloud storage server and revoked cluster users throughout user revocation in the practical cloud storage system. During this paper, we have a tendency to discover the collusion attack within the existing theme and supply associate economical public integrity auditing theme with secure cluster user revocation primarily based on vector commitment and verifier-local revocation cluster signature. The overall security in cloud and experimental analysis show that compared with its relevant themes in our scheme is additionally secure and economical [13].

Keywords: Cloud Service Provider, Public Auditing, Auditing Protocol, Batch Auditing, Privacy-Preserving,

1. Introduction

Cloud computing is an Internet based computing processing structure, where virtually shared servers will provide software, infrastructure, and presenting to customers on a pay as you use structure. It allows the users to access admittance of the information from anywhere and anytime. The systems in cloud architecture are involved in the delivery of cloud computing. It generally involves in the process multiple cloud components will communicate with each other over application programming interfaces, usually web services. Cloud security does not change its approach on how to manage security from avoiding them to detective and corrective actions.

It organizes however, to give you the ability to perform these activities in a more active manner [12]. User data is secured within data centers and where some countries require data to be stored in their country, by choosing a provider that has multiple data centers across the world can help to achieve this. Though the Cloud Service Provider gives the privacy and integrity of the data, this tracks these actual usages of the user’s data in the cloud by using novel highly decentralized framework data and policies. An object-centred approach that enables enclosing our logging mechanism together with users’ data and policies. By leveraging the Java Archive programmable capabilities to both create a dynamic and traveling object. To strengthen user’s control, also provide distributed auditing mechanisms. Infrastructure is offloaded to cloud providers while security becomes a shared responsibility between the cloud service provider and the enterprise tenant. Fortinet permits assignments in public cloud to ensure privacy and confidentiality [10].

2. Related Work

Cloud storage has been studied in recent years as one of the hot spots in cloud computing. Many branches of cloud storage, such as data auditing, privacy preservation, and dynamic updating, are the subject of intense discussion as well. For data auditing in a cloud, many protocols have been proposed in the past few years and can be divided into private protocols and public protocols. The private auditing protocols, the participating entities are the data owner and the Cloud Service Provider. Only the data owner possesses the private key, and the entire auditing process is executed by the owner. A suitable relationship between the doubly linked info table and the location array makes our protocol perform well both in terms of effective dynamic support and compact overhead. Besides, certain basic experiments in cloud auditing, such as batch auditing, block less verification and indolent update have been overcome by our protocol. Third party auditor is used evaluate the service quality from an objective and the self-governing perspective [7].
Qian Wang et. al., used this well-known classification technique to classify auditing in cloud computing. They run this method on an apache Hadoop environment that of course uses the MapReduce paradigm to process on big data. Public adaptability too permits clients to delegate the integrity proof tasks to third party auditing while they themselves can be unreliable or not be able to commit necessary computation resources performing the continuous verifications. The additional major concern is how to construct the of confirmation protocols, so they can accommodate dynamic data files. They explored the problem of providing simultaneous public auditability and data dynamics for remote data integrity check. Their construction is deliberately designed to meet these two important goals. In mean

while efficiency being kept closely in mind to attain a well-organized data dynamics, they improve the current proof of storage models by employing the classic Merkle hash tree construction for block tag authentication [1].

Jian Liu et. al., used a public auditing scheme for the regenerating-code-based cloud storage system, where the data owner are privileged to delegate third party auditor for their data validity checking the public auditing scheme for the regeneration code-based cloud storage system, where the data owners are privileged to delegate Third party auditing for their data validity checking. To protect the original data privacy against third party auditors, they randomize their coefficients in the commencement rather than applying the blind technique during the auditing process. The data owner cannot always stay online in practise, in order to keep the storage available and verifiable after a malicious corruption. They introduced a semi-trusted proxy into the system model and provide an honour for the proxy to handle the compensation of the coded blocks and authenticators [3].

Zhihua Xia et. al., used a safe, effective and dynamic search system is proposed in which supports not only the correct multi-keyword ranked search but also the dynamic deletion and insertion of documents. They build an extraordinary keyword balanced binary tree as the index, and propose a Greedy Depth-First Search algorithm to obtain better efficiency than linear search. It Give parallel search process can be carried out to reduce time cost. The security of the scheme is protected against two threat models by using the secure k-nearest neighbour’s algorithm. The data owner needs to store the unencrypted index tree and the information that is necessary to recalculate the inverse document frequency values. Such an active data owner may not be very suitable for the cloud computing model. It could be a meaningful, but difficult future work to design a dynamic, searchable encryption scheme whose updating operation can be completed by a cloud server only, meanwhile reserving the ability to support multi-keyword ranked search process [4].

Zhangjie Fu et. al., used a statement of problem of personalized address the problem of personalized, multi-keyword ranked search over encrypted cloud data. By seeing the user search history, we build a user interest model for individual users with the help of semantic ontology word net. They have studied and solved the problem of personalized multi-keyword ranked search over encrypted data while preserving privacy in cloud computing. With the help of semantic ontology word net, we build a user interest model for individual user by analysing the user’s search history, and adopt a scoring mechanism to express user interest smartly. They have been addressed the limitations of the model of one size fit all and keyword precise search. They proposed two personalized multi-keyword ranked search over encrypted schemes for different search intentions [15]. Wide experiments on their real-world dataset authenticate their analysis and show that our proposed solution is very efficient and effective. The proposed personalized search goals at exploiting user information to permit search results better to meet the individual user’s search purpose. The overall method is to build a user profile, which labels the user’s interests or preferences that can directly set by the user or collected during the search history [5].

Yan Zhu et. al., Implemented a dynamic audit facility for confirming the integrity of an untrusted and outsourced storage. Their audit service is based on the techniques, fragment structure, random sampling, and index-hash table, supporting verifiable updates to outsourced data and timely anomaly detection. They proposed a technique based on probabilistic query and periodic verification for enlightening the performance of audit services. Their experimental results not only authenticate the effectiveness of our approaches, but also show our audit system verifies the integrity with lower computation overhead and the needful less extra storage for audit metadata process [2].

3. Proposed Work

The propose system, a privacy-preserving public auditing mechanism for shared data in the cloud. We utilize ring signatures to construct homomorphism authenticators, so that a public verifier is able to audit
shared data integrity without retrieving the entire data, yet it cannot distinguish who is the signer on each block [8]. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch editing. The proposed architecture has the function of processing of regeneration file in the auditing process. This process consists of i) Traceability, ii) Caesar Cipher, iii) User Revocation.

4. Conclusion

In this paper, we have studied existing solutions to perform the cloud service provider operations in security cloud computing. The future system can achieve several auditing tasks simultaneously. They increase the efficiency of verification for several auditing tasks. Finally, users can request to auditor to get back the corrupted file, while the auditor checks for the file that is corrupted or not and send back the solution for that request. The future work has been eligible to give high security to the data [14].

References


