International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 06
May 2017

Privacy Preserving Secure Public Auditing By Traceability System

GUNDIPAGA RAJA RATNA KIRAN [1] & MR. B. LAXMAIAH [2]
[1]M-Tech Dept. of CSE Sarada Institute of Science and Technology, Khammam,
Mail id: grrkiran@gmail.com
[2]HOD & Associate Professor Dept. of CSE Sarada Institute of Science and Technology, Khammam

Abstract

When we are utilizing cloud storage accommodation, it is possible for data to be not only stored in the cloud, but with all can shared across multiple users. It's a sizably voluminous challenge is to preserve identity privacy of public auditing for such shared data. It sanctions public auditing on shared data stored in the cloud by this first privacy preserving mechanism. For auditing the integrity of shared data it utilizes the ring signature to compute the verification information. The third party auditor is able to verify the integrity of shared data in the cloud. Hence, this is the mechanism who kept the identity of signer in shared data private from third party auditor. By utilizing the auditing shared data it demonstrates efficacy and efficiency.

Keywords: Cloud computing, Public auditing, Privacy-preserving, Shared data, Third Party Auditor.

1. INTRODUCTION

In this model, privacy is accomplished by sanctioning heartiest up load their data in multi clouds and data is split into multiple components so it gives more bulwark. Current working scenario involves paper predicated work for Data analysis and verification. Data Storage is one way to mitigate the privacy concern. Unauthorized users can leakorm is utilize the data, this quandary still remains due to the paper predicated work. We propose Oruta, a privacy preserving public auditing mechanism. We utilize ring signatures to construct homo morphic authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer in shared data is kept private from the public verifier. In integration, this mechanism used to fortify batch auditing, which can perform multiple auditing tasks simultaneously and ameliorate the efficiency of verification.

Cloud Computing is the dreamed vision of computing as a public utility. It is a model

for enabling convenient, on demand network access to shared pool of configurable computing resources (e.g. networks, servers, storage, application and accommodations) that can be rapidly provisioned and relinquished with minimal management effort or accommodation provider interaction. A cloud provider is a company which hosts the servers on its premises and makes the accommodations available on demand. The ever more frugal and more puissant processors, together with the "software as a service" (SaaS) computing architecture, are transforming data centers into pools of computing accommodation on a sizably voluminous scale. Meanwhile, the incrementing network bandwidth and reliable yet flexible network connections make it even possible that clients can now subscribe high-quality accommodations from data and software that reside solely on remote data centers. The construction of cloud and storing data in it has tremendous benefits. It facilitates the authenticated and sanctioned cloud users to access cyclopean resources that are outsourced and shared in the cloud.

In cloud storage, consistency not only determines correctness but additionally the genuine cost per transaction. In this work to solve the above privacy issue on shared data, we propose Oruta, a novel privacy-preserving public auditing mechanism. More categorically, we utilize ring signatures [8] to construct homomorphic authenticators [9] in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data—while the identity of the signer on each block in shared data is kept private from the public verifier. In integration, we further elongate our mechanism to fortify batch auditing, which can perform multiple auditing tasks simultaneously and ameliorate the efficiency of verification for multiple auditing tasks. Meanwhile, Oruta is compatible with arbitrary masking [10], which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we withal leverage index hash tables from a precedent public auditing solution [09] to fortify dynamic data.

2. RELATED WORK

Existing System:

Many mechanisms have been proposed to sanction not only a data owner itself but additionally a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing. In these mechanisms, data is divided into many minute blocks, where each block is independently signed by the owner; and a desultory coalescence of all the blocks in

lieu of the whole data is retrieved during integrity checking. A public verifier could be a data utilizer (e.g., researcher) who would relish to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking accommodations.

Moving a step forward, Wang et al. designed an advanced auditing mechanism .so that during public auditing on cloud data, the content of private data belonging to a personal utilizer is not disclosed to any public verifiers. Haplessly, current public auditing solutions mentioned above only fixate on personal data in the cloud .We believe that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage. Therefore, it is withal obligatory to ascertain the integrity of shared data in the cloud is veridical.

Subsisting public auditing mechanisms can authentically be elongated to verify shared data integrity. However, an incipient paramount privacy issue introduced in the case of shared data with the utilization of subsisting mechanisms is the leakage of identity privacy to public verifiers.

Disadvantages of Existing System:

Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers. Protect this confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing.

A. Proposed System:

In this paper, to solve the above privacy issue on shared data, we propose Oruta, a novel privacy-preserving public auditing mechanism More concretely, we utilize ring signatures to construct homomorphic authenticators in Oruta, so that a public verifier is able to verify the integrity of shared data without retrieving the entire data while the identity of the signer on each block in shared data is kept private from the public verifier. In integration, we further elongate our mechanism to fortify batch auditing, which can perform multiple auditing tasks simultaneously and amend the efficiency of verification for multiple auditing tasks. Meanwhile, Oruta is compatible with desultory masking, which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we additionally leverage index hash tables from an anterior public auditing solution to fortify dynamic data. A high-level comparison among Oruta and subsisting mechanisms is presented.

Advantages of Proposed System:

A public verifier is able to correctly verify shared data integrity. A public verifier

cannot distinguish the identity of the signer on each block in shared data during the process of auditing. The ring signatures generated for not only able to preserve identity privacy but also able to support block less verifiability.

3. IMPLEMENTATION

Cloud Assistant:

In the first module, we design our system with Cloud Server, where the datas are stored ecumenically. Our mechanism, Oruta, should be designed to achieve following properties:

(1) Public Auditing: A public verifier is able to publicly verify the integrity of shared data without retrieving the entire data from the cloud.

(2) Correctness: A public verifier is able to correctly verify shared data integrity.

(3)Unforgeability: Only a utilizer in the group can engender valid verification metadata (i.e., signatures) on shared data.

(4) Identity Privacy: A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.

Crowd of Customers:

There are two types of users in a group: the pristine utilizer and a number of group users. The pristine utilizer initially engenders shared data in the cloud, and apportions it with group users. Both the pristine utilizer and group users are members of the group. Every member of the group is sanctioned to access and modify shared data. Shared data and its verification metadata (i.e., signatures) are both stored in the cloud server. A public verifier, such as a third party auditor providing expert data auditing accommodations or a data utilizer outside the group intending to utilize shared data, is able to publicly verify the integrity of shared data stored in the cloud server.

Owner Registration: In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be capable of doing it. For that he requires to fill the details in the registration form. These details are maintained in a database. Owner Authenticate: In this module, owner have to authenticate, they should authenticate by giving their electronic mail id and password. Utilizer Registration: In this module if a utilizer wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database. Utilizer Authenticate: If the utilizer is a sanctioned utilizer, he/she can download the file by utilizing file id which has been stored by data owner when it was uploading.

Social verifier:

When a public verifier wishes to check the integrity of shared data, it first sends an auditing challenge to the cloud server. After receiving the auditing challenge, the Cloud server responds to the public verifier with an auditing proof of the possession of shared data. Then, this public verifier checks the correctness of the entire data by verifying the correctness of the auditing proof. Essentially, the process of public auditing is a challenge and- replication protocol between a public verifier and the cloud serve

Scrutinize Module:

In this module, if a third party auditor TPA (maintainer of clouds) should register first. This system sanctions only cloud accommodation providers. After third party auditor gets authenticated in, He/ She can optically discern how many data owners have uploaded their files into the cloud. Here we are providing TPA for maintaining clouds. We only consider how to audit the integrity of shared data in the cloud with static groups. It signifies the group is pre-defined afore shared data is engendered in the cloud and the membership of users in the group is not transmuted during data sharing. The pristine utilizer is responsible for deciding who is able to apportion her data afore outsourcing data to the cloud. Another intriguing quandary is how to audit the integrity of shared data in the cloud with dynamic groups an incipient utilizer can be incorporated into the group and a subsisting group member can be revoked during data sharing while still preserving identity privacy.

4. EXPERIMENTAL RESULTS

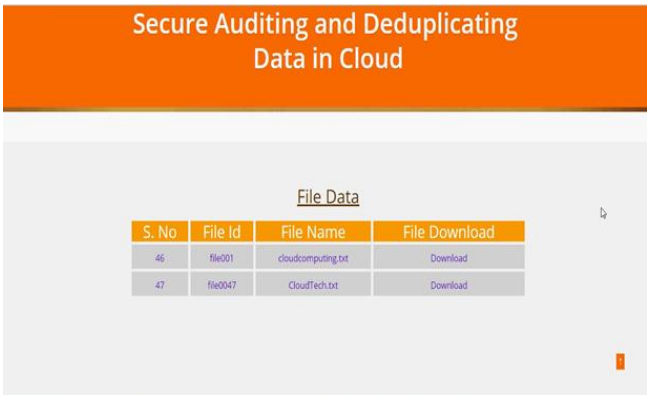

Fig 1: Files Data

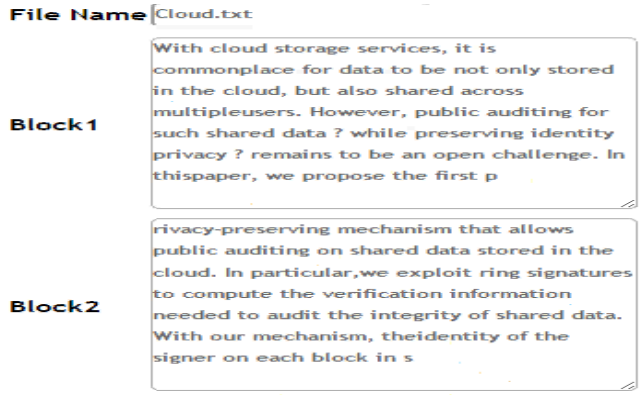

Fig 2: Uploaded File divided into blocks.

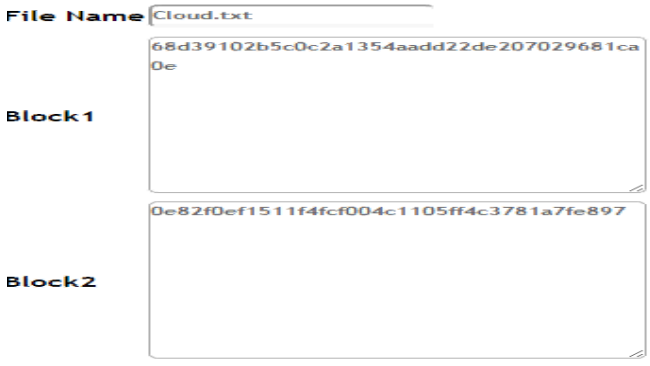

Fig 3: Stored Files Decrypted Form

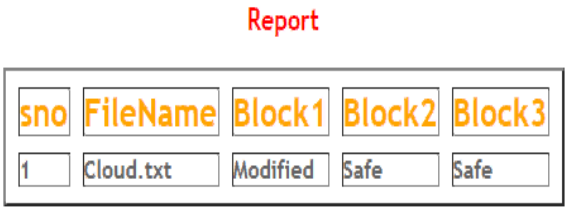

Fig 4: File Status with blocks in Cloud.

5. CONCLUSION

To ascertain cloud data storage security, it is critical to enable a TPA to evaluate the accommodation quality from an objective and independent perspective. Public audit ability additionally sanctions clients to delegate the integrity verification tasks to TPA while they themselves can unreliable or not be able to commit indispensable computation resources performing perpetual verifications. In this paper, we reviewed sundry privacy preserving mechanisms for static group in cloud computing and propose an incipient conception for identity privacy with efficient utilizer revocation in cloud computing environment. This paper category the methodologies in the literature as encryption predicated methods, access control predicated mechanisms, query integrity/keyword search schemes, and auditability schemes. Even though there are many techniques in the literature for considering the concerns in privacy, no approach is highly developed to give a privacy-preserving storage that surmounts all the other privacy concerns. Thus to handle all these privacy concerns, we require to develop privacy–preserving framework which handle all the worries in privacy security and reinforce cloud storage accommodations.

6. 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,‖ Communication softhe ACM, vol. 53, no. 4, pp. 50–58, Apirl 2010.

[2]G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner,Z.Peterson,andD.Song,―ProvableDataPossessionatUntrustedStores,inProc. ACMConferenceonComputer and Communications Security(CCS), 2007,pp. 598–610.

[3]C.Wang, Q.Wang, K.Ren, andW.Lou,―Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, ―How to Leak a Secret, in Proc. International Conference on the Theory and Application of Cryptology and Information Security(ASIACRYPT).Springer Verlag, 2001, pp. 552–565.

[5]D. Boneh, C. Gentry, B.Lynn, and H.Shacham, ―Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques(EUROCRYPT).Springer-Verlag,2003,pp.416–432.

[6] H.Shachamand, B.Waters,―Compact Proofs of Retrievability in Proc. International Conference on theTheory and Application of Cryptology and Information Security (ASIACRYPT). Springer Verlag, 2008, pp. 90–107.

[7]Y.Zhu, H.Wang,Z.Hu, G.-J.Ahn, H.Hu, andS.S.Yau,―Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds ,in Proc. ACM Symposium on Applied Computing(SAC), 2011, pp. 1550–1557.

[8] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", Prepared for the World Privacy Forum, online at http://www.worldprivacyforum.org/pdf/WPF Cloud Privacy Report.pdf, Feb 2009.

[9] W. Itani, A. Kayssi, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing architectures," Eighth IEEE International Conference on Dependable, Autonomic and SecureComputing, Dec 2009.

[10] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, online at http://www.cloudsecurityalliance.org.

Authors Profile

GUNDIPAGA RAJA RATNA KIRAN

B-Tech in Sarada Institute Of Technology And Science, Khammam, percentage in May 2012. M-Tech Computer Science And Engineering from Sarada Institute of Science and Technology (SITK), Khammam.

MR. B. LAXMAIAH

Working as Head of the Department, Associate professor CSE, Sarada Institute of Technology & Scinece (SITS), Khammam. He obtained M-Tech degree from JNTUH, Hyderabad. His research areas include Object Oriented Programming Througt Java, Data base Management System, Data Structures, Web Services, Data Warehousing and Data Mining and Operating Systems.