GE-International Journal of Engineering Research
Vol. 3, Issue 9, Sep 2015 IF- 4.007 ISSN: (2321-1717)
© Associated Asia Research Foundation (AARF) Publication
Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

PRIVACY-PRESERVING PUBLIC AUDITING FOR SHARED DATA IN THE CLOUD

Mr. CH. Narasimha Rao, (P.G. Scholor)

Mr. N. Venkatadri, (Assoc.Prof, SKR Engg College, Manubolu)

ABSTRACT

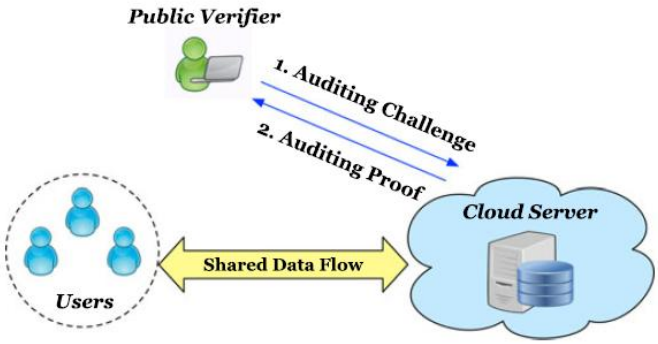
Cloud knowledge services is provided, commonplace for maintain knowledge to be not solely hold on within the cloud. Knowledge additionally shared across multiple users within the cloud.

In addition, our mechanism is in a position to perform multiple auditing tasks at the same time rather than corroboratory them one by one. Our experimental results demonstrate the effectiveness and potency of our mechanism once auditing shared knowledge integrity. many mechanisms are designed to permit each knowledge homeowners and public verifiers to with efficiency audit cloud knowledge integrity while not retrieving the whole knowledge from the cloud server. sadly, the integrity of cloud knowledge is existence of hardware and code failures and human errors are increased. However, public auditing on the integrity of shared knowledge with these existing mechanisms can inevitably reveal steer identity privacy to public verifiers. This paper is maintaining to the novel privacy conserving mechanism it's supporting to the general public auditing on shared knowledge hold on within the cloud. during this mechanism we have a tendency to exploit ring signatures are verified to the whole information required to audit the correctness of shared knowledge. Main aim is initial check the full knowledge each block public supporter shared knowledge within the cloud and ring signatures are verified to the actual authentication public verifiers while not retrieving entire knowledge within the entire file. Our mechanism is in a position to activity to the multiple auditing tasks at the same time of corroboratory them one by one. Our experimental results demonstrate the effectiveness and potency of our mechanism once auditing shared knowledge integrity. Cloud is principally dada is hold on isn't solely the one place relying it's self .Public verifiers will produce the GROUP1 and GROUP2 choices our alternative. during this method is principally login and sign to the choose

the teams. each cluster users transfer one file and than generate the one key each file secret's distinct. it's additionally file deletion and states checking everything is maintain the correct ring signatures initial verifiers to the general public auditing users. each cluster user secret's send to the present their mail address. therefore this mechanism additionally referred to as knowledge is secured and privacy conserving is maintained and public auditing by the general public users.

Key Terms: Public Auditing, Privacy Preserving, Shared data, Cloud Computing

SYSTEM ARCHITECTURE:



EXISTING SYSTEM:

Many mechanisms have been proposed to allow not only a data owner itself but also 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 small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead of the whole data is retrieved during integrity checking . A public verifier could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services.

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 user is not disclosed to any public verifiers. Unfortunately, current public auditing solutions mentioned above only focus on personal data in the cloud .We believe that sharing data among multiple users is perhaps one of the most engaging features that motivates cloud storage. Therefore, it is also necessary to ensure the integrity of shared data in the cloud is correct.

Existing public auditing mechanisms can actually be extended to verify shared data integrity. However, a new significant privacy issue introduced in the case of shared data with the use of existing mechanisms is the leakage of identity privacy to public verifiers.

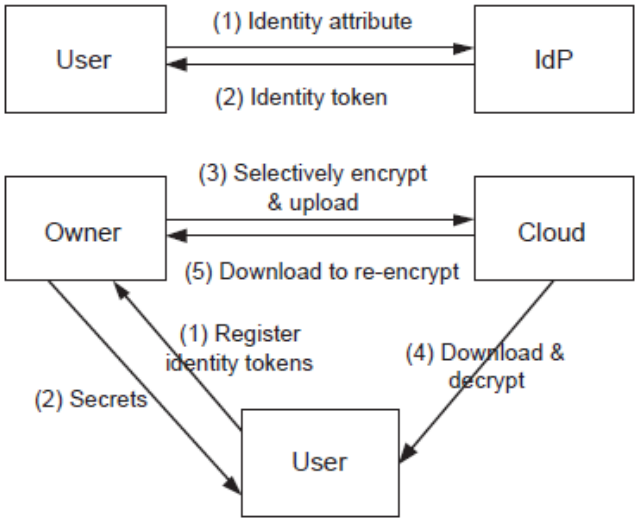
DISADVANTAGES OF EXISTING SYSTEM:

I. Failing to preserve identity privacy on shared data during public auditing will reveal significant confidential information to public verifiers.

II. Protect these confidential information is essential and critical to preserve identity privacy from public verifiers during public auditing.

As future enhancement, we enhance the Oruta system in two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected, the current design of ours does not support traceability. To the best of our knowledge, designing an efficient public auditing mechanism with the capabilities of preserving identity privacy and supporting traceability is still open. Another problem for our future work is how to prove data freshness (prove the cloud possesses the latest version of shared data) while still preserving identity privacy.

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 specifically, 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 addition, we further extend our mechanism to support batch auditing,

which can perform multiple auditing tasks simultaneously and improve the efficiency of verification for multiple auditing tasks.

- ✓ Meanwhile, Oruta is compatible with random masking, which has been utilized in WWRL and can preserve data privacy from public verifiers. Moreover, we also leverage index hash tables from a previous public auditing solution to support dynamic data. A high-level comparison among Oruta and existing mechanisms is presented.

ADVANTAGES OF PROPOSED SYSTEM:

1. A public verifier is able to correctly verify shared data integrity.
2. A public verifier cannot distinguish the identity of the signer on each block in shared data during the process of auditing.
3. The ring signatures generated for not only able to preserve identity privacy but also able to support blockless verifiability.

There are 4 Types of Modules are there:

- ➢ Cloud server
- ➢ Group of users
- ➢ Public verifier
- ➢ Auditing Module

Cloud server

- ✓ In the first module, we design our system with Cloud Server, where the datas are stored globally. 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 user in the group can generate 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.

Group of users

- ✓ There are two types of users in a group: the original user and a number of group users. The original user initially creates shared data in the cloud, and shares it with group users. Both the original user and group users are members of the group. Every member of the group is allowed 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 thirdparty auditor providing expert data auditing services or a data user 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 able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.
- ✓ Owner Login: In this module, owner have to login, they should login by giving their email id and password.
- ✓ User Registration: In this module if a user 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.
- ✓ User Login: If the user is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

Public 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- response protocol between a public verifier and the cloud server

Auditing Module

- ✓ In this module, if a third party auditor TPA (maintainer of clouds) should register first. This system allows only cloud service providers. After third party auditor gets logged in, He/ She can see 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 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. Another interesting problem is how to audit the integrity of shared data in the cloud with *dynamic groups* — a new user can be added into the group and an existing group member can be revoked during data sharing — while still preserving identity privacy.

CONCLUSION

In this, we propose a privacy-preserving public auditing mechanism for shared data in the cloud. We are maintaining 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. To improve the efficiency of verifying multiple auditing tasks, we further extend our mechanism to support batch auditing. There are two interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations. Since Oruta is based on ring signatures, where the identity of the signer is unconditionally protected the current design of ours does not support traceability.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[10] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data

[2] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[3] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[5] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[6] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[7] The MD5 Message-Digest Algorithm (RFC1321). https://tools. ietf.org/html/rfc1321, 2014.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS'09), pp. 1-9, 2009.

[12] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network

Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop (CCSW'10), pp. 31-42, 2010.

[14] C. Wang, S.S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[15] B. Wang, B. Li, and H. Li, "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," Proc. IEEE INFOCOM, pp. 2904-2912, 2013.