ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Ring signatures based framework for verification of shared data in Cloud Computing Environment.

Vutlapalli Anil Kumar
MTech Student
Department of Computer Science Engineering
Chilukur Balaji Institute Of Technology

P. Dharshan
Associate Professor & HOD,
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

G.Thirupathi Reddy
Assitant Proffessor
Department of Computer Science Engineering,
Chilukuri Balaji Institute of Technology.

Abstract: ***Cloud computing provides an economical and efficient solution for sharing data among the cloud users with low maintenance. There is still a challenging issue, due to the frequent change of the membership for sharing data in a multi-owner manner while preserving data and identity privacy from an un-trusted cloud. The public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data. The signatures to compute the verification information needed to audit the integrity of shared data. In TPA, who is still able to publicly verify the integrity of shared data without retrieving the entire file is identified. The ring signature scheme is needed to audit the correctness of shared data. With this mechanism, the identity of the signer on each block in shared data is kept secret or private from public verifiers. Public verifiers are one who are able to efficiently verify shared data integrity without retrieving the entire file.***

Keywords: ***Cloud, Signature verification, Data Storage, Data sharing, TPA, Audit.***

Introduction:

Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services.

Cloud computing, or in simpler shorthand just "the cloud", also focuses on maximizing the effectiveness of the shared resources. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users. For example, a cloud computer facility that serves European users during European business hours with a specific application (e.g., email) may reallocate the same resources to serve North American users during North America's business hours with a different application (e.g., a web server). This approach should maximize the use of computing power thus reducing environmental damage as well since less power, air conditioning, rack space, etc. are required for a variety of functions. With cloud computing, multiple users can access a single server to retrieve and update their data without purchasing licenses for different applications.

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Cloud storage services may be accessed through a co-located cloud computer service, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Cloud storage is based on highly virtualized infrastructure and is like broader cloud computing in terms of accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Cloud storage services can be utilized from an off-premises service or deployed on-premises.

Cloud storage typically refers to a hosted object storage service, but the term has broadened to include other types of data storage that are now available as a service, like block storage.

Object storage services like Amazon S3 and Microsoft Azure Storage, object storage software like Openstack Swift, object storage systems like EMC Atmos and Hitachi Content Platform, and distributed storage research projects like OceanStore[5] and VISION Cloud [6] are all examples of storage that can be hosted and deployed with cloud storage characteristics.

Cloud storage is:

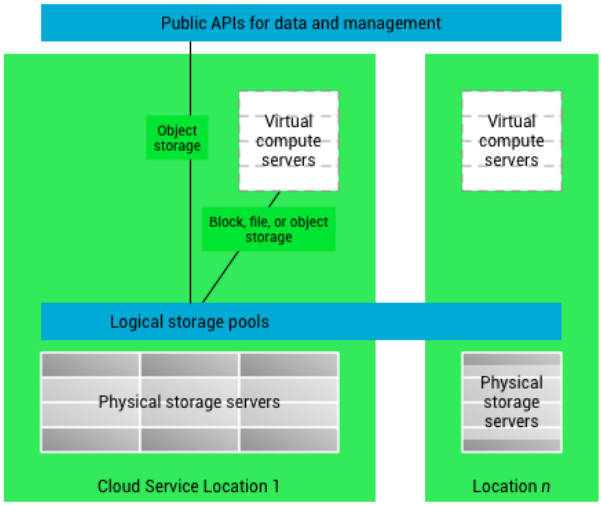
Made up of many distributed resources, but still acts as one - often referred to as federated storage clouds

Highly fault tolerant through redundancy and distribution of data

Highly durable through the creation of versioned copies

Typically eventually consistent with regard to data replicas

High level cloud storage 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:

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

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

Proposed System:

- In this paper, to solve the above privacy issue on shared data, we propose Oruta, a novel privacy-preserving public auditing mechanism.

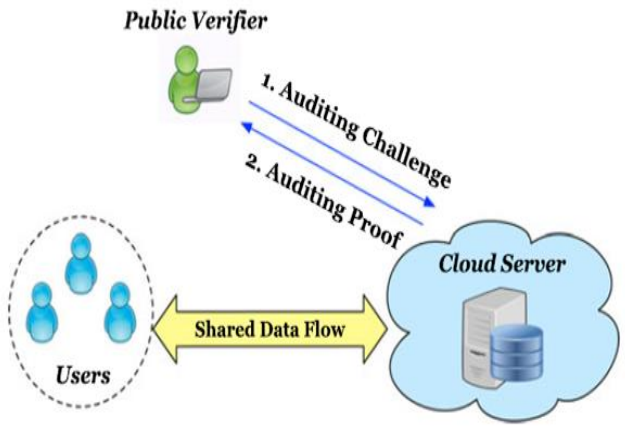
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- 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.

System Architecture:



Overview Of Proposed System

- Public Auditing: A public verifier can able to publicly verify the integrity of shared data without retrieving the whole data from the cloud.
- Correctness: A public verifier is able to correctly verify shared data integrity and correctness.
- Unforgeability: Only a user in the group can generate valid verification code (i.e., signatures) on shared data.
- Identity Privacy: A public verifier cannot differentiate the identity of the signer on each block in shared data during the process of auditing.

Conclusion

In this paper, the studied and implemented Oruta method is used to share data in the cloud. Oruta is a privacy-preserving public auditing mechanism. We utilize ring signatures to construct homomorphic authenticators, so that a public verifier is able to audit shared data integrity without retrieving the entire data. The oruta scheme cannot differentiate the signer on each block. To improve the efficiency of verifying multiple auditing tasks, the ORUTA scheme extended to support batch auditing.

References:

[1] Boyang Wang, Baochun Li, and Hui Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud"IEEE TRANSACTIONS ON CLOUD COMPUTING,VOL. 2,NO. 1,JANUARY-MARCH 2014.

[2] 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, Communications of the ACM", vol. 53, no. 4, pp. 5058, April 2010

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song," Provable Data Possession at Untrusted Stores, in Proc. ACM Conference on Computer and Communications Security (CCS)", 2007, pp. 598610.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[4] 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.525533.

[5] 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)". SpringerVerlag, 2001, pp. 552565.

[6] 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.416432.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability,in Proc. International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT)". SpringerVerlag, 2008, pp. 90107.

[8] 7. M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocolsand Atomic Proxy Cryptography, inthe Proceedings of EUROCRYPT 98".Springer-Verlag, 1998, pp. 127144.

[9] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S.Yau, "Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds, in Proc. ACM Symposium on Applied Computing (SAC)", 2011, pp.15501557