Enabling Public Verification for Secure Distributed Data in the Cloud

Kakkerla Shivakumar
Assistant Professor, Department of CSE Geethanjali College of Engineering & Technology, Hyderabad, Telangana, INDIA

***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. Here, a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud has been proposed. Any cloud user can anonymously share data with others by providing group signature and dynamic broadcast encryption techniques. Meanwhile, the storage overhead and encryption computation cost of the scheme are independent with the number of revoked users.**

***Index Terms*- Cloud Server, Privacy Preserving Access Control, Attribute-Based Encryption.**

I. INTRODUCTION

Cloud concept is nothing but the storage service, but it can also share across multiple users. we firstly prioritizes privacy preserving mechanism because while auditing data from cloud services it's not a secured while that private information is publicly protected by cloud service. Specifically, the group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users which protects the confidentiality from the revoked users in the dynamic broadcast encryption scheme. We propose that while any user is accessing the data from cloud it must be secured by unauthorized person or hacker. Cloud is un-trusted file storage, so we utilize encryption based access control for sharing document in the cloud storage service. User's data is encrypted by using cryptographic technique because unauthorized person can hack the user's private data. In this cryptographic technique we uses different algorithms like signature algorithm, key generation algorithm, ring verify algorithm, etc. these algorithms are used in the cryptographic technique. Users can enjoy high-quality services by migrating local data management systems into cloud servers.

II. LITERATURE SURVEY

A. Privacy-Preserving In the Cloud

In the Existing system, cloud environment provides large space for storing and managing information for the internet application. The TPA is also important mechanism for authentication is done by this system. The TPA verifies the valid and invalid user by evaluating user identity attributes but if the TPA get hacked by some another then the user not get any notification from cloud due to this users may losses the irrivate information or leakage, so this is big drawback of the existing system. In the previous system, for security purpose OTP (one time password) is not generated while the user's verification is done.

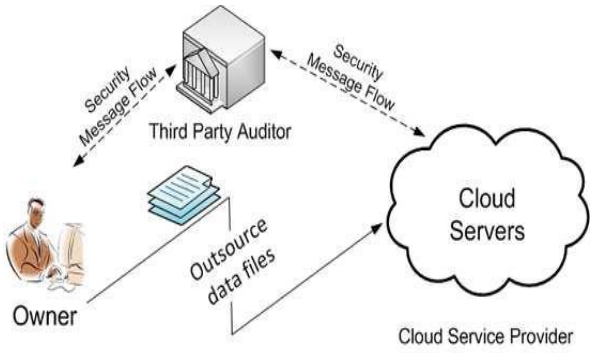

Figure1- System Model Includes The Cloud Server, The Third Party Auditor And Users

Due to the lack of knowledge of decryption keys, the unauthorized users as well as storage servers cannot learn the content od data files. A secure provenance scheme based on the cipher text policy attribute based encryption technique proposed by Lu et al.[3] by setting group with a single attribute. The Deffie-Hellman-key Exchange algorithm is used in previous system. But this is very risky because in this algorithm the man-in-middle-attack was generated so

Deffie-Hellman-key Exchange algorithms issueless. In the previous system encryption and decryption is done by common protection method so it's easy to the hacker by hack user's private information so the service provider build the firewall for security.

III. RELATED WORK

A. Privacy-Preserving Public Auditing For Shared Data In The Cloud

In proposed system, we provide Security services including authentication, confident ability and integrity provide in cloud system. In this system we are developed users privacy. The users want to share data from the server then it has insecurity between user and server so TPA application will provide the security to user while he getting the information from the cloud server. The TPA will help us to verify the user's correct details and authentication to the server and verifier is able to publicly audit integrity of data without retrieving the entire data.

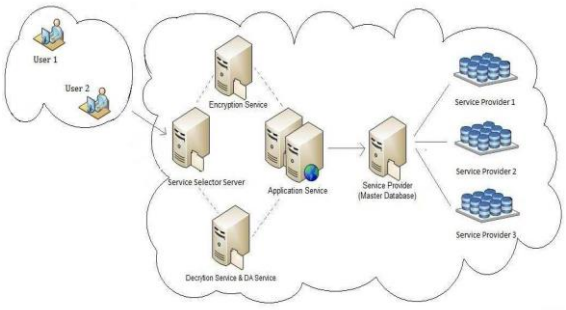

Figure 2- System Architecture

There are number of users who wants to shared their data from cloud server while they sharing their data first he has to collect the private key and public key have public key) from the cloud served the TPA will help us to verify users identity attributes and encrypt it and stored. Scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately The single adoption of their scheme into the case, where any user is granted to store and share data.

While another user want to access the identity by using their mail id. The TPA will check the requested mail id by verifying their main mobile number by OTP (one time password).then encrypted data will decrypt by using the TPA and send to the requested user. During encryption and decryption the RC6 algorithm are used. And while public key and private generating that time SPEKE algorithm are used.

IV. SYSTEM ARCHITECTURE

A. Holomorphic Authenticable Ring Signature:

How to preserve the users Identity attributes from the TPA because the TPA gets hacked by hacker then it may be leakage the users private information so we gave the protection to the server, while it get hack then it will give notification to the user. And again TPA will get ready to another new user.

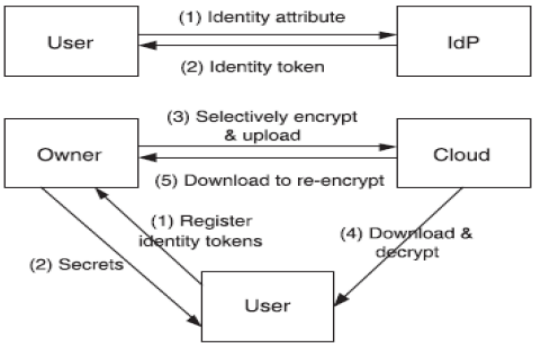

Figure 3. Overall System Architecture

We utilize the ring signature, to construct the shared data. The identity of the signer kept private from the TPA identity attributes. The ring signature is computing the group member's private key but the verify able to determine exact key. Holomorphic authentication has unforgebility (only a user with a private(one user have private key and multiple user it into the different databases in the cloud between this process single-owner manner hinders the case, where any user is granted to store and share data shared data it will request to the server then TPA verifies their decryption the RC6 algorithm are used algorithm are used.

The Holomorphic authentication also satisfy block less verification and non-malleability. Holomorphic authentication ring signature (HARS) utilize the Key generation (Each user has private key or public key), Ring signature a user must be sign on his public key or private key, Ring verify to verify the given block is within the group member.

IV. CONCLUSION

In this paper, we propose Oruta, the first privacy-preserving public auditing mechanism for shared data in the cloud. With Oruta, the TPA is responsible for to audit the integrity of shared data, till cannot distinguish who is the signer on each block which can preserve identity privacy for users. We utilizing, privacy preserving who shared the data in the cloud storage service with the help of the ring signature and

Holomorphic authentication ring signature. And we utilize ring signature to construct the HARS, so TPA will protected from unauthorized user. It will easily audit the integrity of shared data. Our future work is how to audit shared data with dynamic members while users sharing the data it will be safe from the TPA. An interesting problem in our future work is how to efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor.

REFERENCES

[1] Toward Securing Untrusted Storage without Public Key Operations. Dalit Naor IBM Haifa Research Lab Tel Aviv, Israel dalit@il.ibm.com

[2] Rongxing Lu†, Xiaodong Lin‡, Xiaohui Liang†, and Xuemin (Sherman) Shen† Ciphertext-PolicyAttribute-Based Encryption: An Expressive, E_cient, and Provably Secure Realization. BrentWaters _ University of Texas at Austin

[3] Vipul Goyal, Omkant Pandeyy, AmitSahaizBrent Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data".