A SURVEY ON PUBLIC AUDITING FOR GROUP SHARED DATA WITH EFFICIENT USER REVOCATION IN CLOUD

ATHMARAM KURAPATI, M.Tech (CSE), Priyadarshini Institute of Technology & Management

K.KIRAN KUMAR, Associate Professor (Dept.of CSE), Priyadarshini Institute of Technology & Management

ABSTRACT:

Many users are attracted to the cloud, in order to save their cost and to avoid local burden all users are motivated to outsource their data to the cloud, using data service the users can easily store, modify and they can share data as a group. But due to security issues most of the data owners are worrying about data integrity, In this paper data owners can share data with group of users but due to security every user in the group before uploading any data to the cloud he need compute the signature and the problem identified is if data owner leaves the group how to allocate signature to the other group members and public auditing are major issues are identified, to handle these two issues we are proposing new novel technique Proxy Authenticator .If any user is revoked from the group the proxy will assign signature to other group member. If membership is changing frequently and re-signs blocks is large proxy revocation handle effectively.

INTRODUCTION:

Cloud providing storage as service and sharing as a service to the users, due to availability of cloud so many users outsourcing data to the cloud. Cloud describes a new supplement, consumption, and delivery model for IT services based on the Internet. It has been envisioned as the next generation information technology (IT) architecture for enterprises, due to its wide range of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk.

As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' outsourced Data. The knowledge integrity of shared data within the cloud should be compromised. Third Party Auditor is quite an inspector. that audits the integrity on the behalf of cloud service supplier while not retrieving total data? It challenges the cloud server for the correctness of knowledge storage whereas keeping no non-public information. To exempt the burden of management of knowledge of the information owner, TPA can audit the information of shopper. It extinguishes the involvement of the shopper by auditing that whether or not her knowledge hold on within the cloud area unit so intact, which may be vital in

achieving economies of scale for Cloud Computing. Then it relinquishes the audit report which might facilitate homeowners to judge the chance of their signed cloud knowledge services, and it'll even be helpful to the cloud service supplier to enhance their cloud primarily based service platform. during this manner, TPA can facilitate knowledge owner likewise as users to form certain that his knowledge area unit safe within the cloud and management are going to be less burdening to the data owner. Therefore, to sanctioning a privacy-preserving third party Auditing protocol, freelance to user revocation, is that the downside we tend to area unit planning to tackle during this paper. Our review is among rare ones to support privacy-preserving public auditing in cloud computing, with a spotlight on user revocation

LITERATURE REVIEW

Techniques used in Public Auditing on Cloud There are some different techniques which used in different auditing mechanisms. This section introduce some the techniques like MAC, HLA etc. which are used for different purposes like data authentication, data integrity in auditing schemes on cloud.

1. MAC Based Solution

This technique used for data authentication. In this mechanism user upload data blocks with MAC and Cloud provider provides Secret key SK to TPA. Here TPA's task is to retrieve data blocks randomly and MAC uses SK to check correctness of data. Limitations of this technique are:

- Online burden to users due to limited use and state full verification.
- Complexity in communication and computation
- Maintaining and updating TPA states is difficult.
- User need to download all the data to recomputed MAC and republish it on CS
- This technique only supports for static data.

2. HLA Based Solution

This technique performs auditing without retrieving data block. HLA is nothing but unforgettable verification meta data that authenticate. It checks integrity of data block by authenticating it in linear combination of the individual blocks. This technique allows efficient data auditing and consuming only constant bandwidth, but its time consuming as it uses linear combination for authentication.

3. Using Virtual Machine

Abhishek Mohta proposed Virtual machines concept which use in case of Software as a Service (SaaS) model of the cloud computing. In this mechanism as shown in Fig when user request CSP for service CSP authenticate the client and provide a virtual machine by means of Software as a service. Virtual Machine (VM) uses RSA algorithm for cryptography, where client encrypt and de-crypt the file. A SHA-512 algorithm is also used for making the message digest and check the integrity of data. This also helps in avoiding unauthorised access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.

APPROACH AND DESIGN

Problem Definition

While using cloud services as data storage and data sharing in a group, Integrity of personal and shared data on cloud and user revocation are major concerns. This paper uses the concept of homomorphic linear authenticator with random masking technique for personal data and Homomorphic authenticable proxy resignature scheme with Panda public auditing mechanism for shared data and user revocation.

METHODOLODY

Privacy-Preserving Public Auditing For Secure Data Storage: Proxy authenticator with random masking technique is used when there is a need of public auditability without retrieving the data blocks. Proxy Authenticators are unforgeable verification metadata which are used to authenticate the integrity of a data block. Proxy authenticator can be aggregated. It is possible to compute an aggregated Proxy authenticator which authenticates a linear combination of the individual data blocks. This scheme uses below algorithms:

- KeyGen: KeyGen is a key generation algorithm that is executed by the user to setup the scheme.
- SigGen: SigGen is executed by the user to produce verification metadata, which may consist of signatures, or other linked information that will be used for executing audit.
- GenProof: GenProof is executed by the CSP to produce a verification of data storage rightness. VerifyProof: is executed by the TPA to audit the verification from the CSP.

CONCLUSION

This paper discusses Privacy preserving public auditing mechanisms, Proxy authenticator with random masking have been used to guarantee that the third party auditor would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage. Proxy authenticable proxy resignature scheme with Panda public auditing mechanism checks shared data integrity along with efficient user revocation. Furthermore, these mechanisms are able to support batch auditing by verifying multiple auditing tasks simultaneously.

REFERENCES:

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing".

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2011.

[3] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and S. Chen, "Dynamic Audit Services for Outsourced Storage in Clouds,"

IEEE Transactions on Services Computing, accepted.

[4] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012

[5] Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976- 8491(Online), June 2012

[6] B. Wang, B. Li, and H. Li, "Panda: Public Auditing For Shared Data with Efficient User Revocation in The Cloud" IEEE Trans. Services Computing, Dec.2013

[7] 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.

[8] 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.

[9] Lakshmi et al., International Journal of Advanced Research in Computer Science and Software Engineering 4(8), August - 2014, pp. 54-62

[10] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," in the Proceedings of EUROCRYPT 98. Springer Verlag, 1998, pp.127–144