Multi Proxy Resignature with Public Auditing of Shared Cloud Data for User Revocation

Ms.K.Valli[1] and Ms.A.Punitha2

Information Technology,Manakula Vinayagar Institute of Technology, Pondicherry university
95valli@gmail.com

Information Technology,Manakula Vinayagar Institute of Technology, Pondicherry university
Asst.professor, Manakula Vinayagar Institute of Technology,Puducherry.

ABSTRACT

In the cloud environment users can easily modify and share data as a group. To ensure shared data integrity can be verified publicly, users in the group need to compute signatures on all the blocks in shared data. Different blocks in Shared data are generally signed by different users due to data modifications performed by different users. For security reasons, once a user is revoked from the group, the blocks which were previously signed by this revoked user must be re-signed by an existing user. The straight forward method, idea of proxy re-signatures which allows an the cloud to re-sign blocks on behalf of existing. In addition, a public verifier is always able to audit the integrity of shared data without retrieving the entire data from the cloud, even if some part of shared data has been re-signed by the cloud. In this design if revoked user is able to collude with the cloud, which possesses a resigning key, then the cloud and the revoked user together are able to easily reveal the private key of an existing user. Propose a novel public auditing mechanism for the integrity of shared data with efficient user revocation in mind. By utilizing the idea of proxy re-signatures, we allow the cloud with collusion resistance which restricts to compute the private key of an existing user.

Index Term— Re-signature, Multiple Auditing, User Revocation, Third party Auditor

1. INTRODUCTION

With data storage and sharing services, such as Google Drive, provided by the cloud, people can easily work together as a group by sharing data with each other. More specifically, once a user creates shared data in the cloud, every user in the group is able to not only access and modify shared data, but also share the latest version of the shared data with the rest of the group. Although cloud providers promise a more secure and reliable environment to the users, the integrity of data in the cloud may still be compromised, due to the existence of hardware/software failures and human errors. To protect the integrity of data in an untrusted cloud, a number of mechanisms have been proposed. In these mechanisms, a signature is attached to each block in data, and the integrity of data relies on the correctness of these signatures. One of the most significant and common features of these mechanisms is their ability to allow not only the data owner, but also a public verifier, such as a third party auditor (TPA), to check data integrity in the cloud without downloading the entire data, referred to as public auditing. Most of the previous works focus on auditing the integrity of personal data. Different from these works, our recent work focuses on how to preserve identity privacy from the TPA when auditing the integrity of shared data. Unfortunately, none of the previous works, including our own, considers the efficiency of user revocation when auditing the correctness of shared data in the cloud. With shared data, once a user modifies a block, she also needs to compute a new signature for the modified block. Due to the modifications from different users, different blocks are signed by different users. For security reasons, when a user leaves the group or misbehaves, this user must be revoked from the group. As a result, this revoked user should no longer be able to access and modify shared data, and the signatures generated by this revoked user are no longer valid to the group.

Therefore, although the content of shared data is not changed during user revocation, the blocks, which were previously signed by the revoked user, still need to be re-signed by an existing user in the group, so that, after the revocation, the integrity of the entire data can still be verified with the public keys of existing users only. Since shared data is outsourced to the cloud and users no longer store it on local devices, the straightforward method to re-compute these signatures during user revocation is to allow an existing user to first download the blocks signed by the revoked user, verify the correctness of these blocks, then re-sign these blocks, and finally upload the new signatures to the cloud. However, this straightforward method may cost the existing user a huge amount of

communication and computation resources by downloading and verifying blocks, and by re-computing and uploading signatures, especially when the number of re-signed blocks is quite large or the membership of the group is frequently changing. To make matters worse, the size of shared data in the cloud is generally large, which further prevents existing users from downloading and re-signing data efficiently.

2. EXISTING SYSTEM

The cloud offers data storage and sharing services to the group. In the group there is one original user and number of group users. The original user creates and shares data with other users in the group through the cloud. The public verifier or third party auditor who can provide verification services on data integrity aims to check the integrity of shared data. To protect the integrity of shared data, allow every user in the group to share a private key and sign each block with it. The idea of proxy re-signature is about when a user is revoked, a new private key need to be securely distributed to every existing user and all the blocks in the shared data have to be resigned with the new private key which is performed by cloud on behalf of existing user, which increases the complexity of key management. Moreover revoked user can able to collude with the cloud and easily reveal the private key of an existing user.

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.

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.

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 decrypt

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 unauthorized access and providing privacy and consistency. Limitation to this technique is it is useful only for SaaS model.

Using EAP

As mentioned by S. Marium Extensible authentication protocol (EAP) can also use through three ways hand shake with RSA. Using EAP they proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) [4]. As compare to SSL authentication protocol APCC is more lightweight and efficient. It also used Challenge – handshake authentication protocol (CHAP) for authentication.

Using Automatic Protocol

Blocker Balkrishna proposed efficient Automatic Protocol Blocker technique for error correction which checks data storage correctness [4].Kiran Kumar proposed automatic protocol blocker to avoid unauthorized access [5]. When an unauthorized user access user data, a small application runs which monitors user inputs, It matches the user input, if it is matched then it allow user to access the data otherwise it will block protocol automatically. It contains five algorithms as keygen, SignGen, GenProof, Verify Proof, Protocol Verifier. Protocol Verifier is used by CS. It contains three phases as Setup, Audit and Pblock.

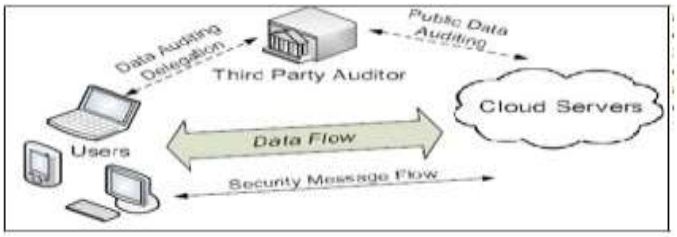

Figure 1. Single re-signature proxy in cloud

3.PROPOSED SYSTEM

A framework of integrity protection on cloud data is presented in Fig., where we can see ensuring data integrity can involve many aspects, ranging from internal and external verifications, data encryption and data anonymization. While this framework is only a wide static overview for the research area, we present a common lifecycle for the detailed dynamic process of a remote integrity verification scheme (with support for dynamic data updates). Security of a public auditing scheme may be jeopardized in every step in the entire auditing process. In the mean time, efficiency of the entire auditing scheme will benefit from efficiency improvement at every step. Therefore, the lifecycle that describes every step of the verification process is essential for analyzing the research problems in this area. The lifecycle can be analysed in the following steps: Setup and data upload; Authorization for TPA; Challenge for integrity proof; Proof integration; Proof verification; Updated data upload; Updated metadata upload; and Verification of updated data. We now analyse in detail how these steps work and why they are essential to integrity verification of cloud data storage.

Propose a multi proxy re-signatures scheme, in which each re signing key divided into pieces and each pieces

distributed to one proxy. These multi proxies belong to same cloud but storage and manage each piece of resigning key independently. Each proxy is able to convert signatures with its own piece when user revocation happens by using homomorphic proxy signature. Multiple auditing is challenging task in Cloud's shared data, which is the process of auditing the multiple block in order to detected polluted blocks in shared data by increasing the number of random selected blocks in single auditing task and generates the proof of all the blocks in cloud by using the bilinear map properties. Complexity of key management in cloud can be reduced by our mechanism, the original user, who performs as the group manager, can keep a short priority list instead of entire list of all the user, which means the cloud able to convert signatures of a revoked user only into one of these short list. Thus our mechanism is able to support multiple auditing tasks and efficient user revocation.

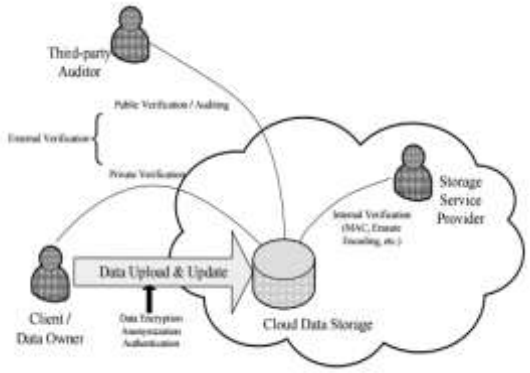

Figure 2. Architecture of of proposed system

4.CONCLUSION

Cloud computing is world's biggest innovation which uses advanced computational power and improves data sharing and data storing capabilities. It increases the ease of usage by giving access through any kind of internet connection. As every coin has two sides it also has some drawbacks. Privacy security is a main issue for cloud storage. To ensure that the risks of privacy have been mitigated a variety of techniques that may be used in order to achieve privacy. This project showcases some privacy techniques and different methods for overcoming the issues in privacy on untrusted data stores in cloud computing. There are still some approaches which are not covered in this project. This project categories the methodologies in the literature as encryption based methods, access control based 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 overcomes all the other privacy concerns. Thus to handle all these privacy concerns, we need to develop privacy preserving framework which handle all the worries in privacy security and strengthen cloud storage services.

.

ACKNOWLEDGMENT

We would like to express our gratitude to all teaching and non-teaching staff members of our department. And above all, the blessings of the Almighty has kept up our spirit and enabled us to complete our study successfully.

REFERENCES

[1] Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE, January/February 2015, vol.8, no. 1. 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, 2012, vol 1, no. 3, pp. 177-183.

[2] 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, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976- 8491(Online), vol. 2, June 2012

[3] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Computer science and Technology, , ISSN: 2229-4333 (Print), March 2012, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940

[4] Jachak K. B., Korde S. K., Ghorpade P. P. and Gagare G. J.,"Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, ISSN. 2249-9423, 12 April 2012, vol. 2, no. 2, pp. 49-52,

[5] J. Yuan and S. Yu, "Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud," in Proceedings of ACM ASIACCS-SCC'13, 2013

[6] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"in the Proceedings of ASIACRYPT 2008. SpringerVerlag,2008,pp.90–107.

[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores,"in the Proceedings of ACM CCS 2007, 2007, pp. 598–610.

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

[9] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-based Secure and Reliable Cloud Storage Service," in the Proceedings of IEEE INFOCOM 2012, 2012, pp. 693–701.

[10]H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing.

[11] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," in the Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.

[12] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," in the Proceedings of ESORICS 2009. SpringerVerlag, 2009,pp.355–370.

