International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 01 | Jan-2016 www.irjet.net p-ISSN: 2395-0072

Survey On: Auditing Public Clouds

Pooja C. Ahirrao[1], Dhanashri V. Pakhale [2], Payal S. Yeola[3],

Prof. Mr.S.R.Lahane[4]

[1] BE Student, Computer Department, GHRHSCOE, Maharashtra, India
[2] BE Student, Computer Department, GHRHSCOE, Maharashtra, India
[3] BE Student, Computer Department, GHRHSCOE, Maharashtra, India
[4] Assistant Professor, Computer Department, GHRHSCOE, Maharashtra, India

---

Abstract – In a Cloud, data storing and sharing is easily modify by user and share a data in a group. To verify shared data integrity and insure publicly, users in a group calculate signature on all the blocks shared data. In a straightforward method, they allows an existing user to download the corresponding part of shared data and resign it during user revocation. It is not sufficient due to of larger size of sharing data in a cloud. Different blocks of sharing data are generally signed by a different users due to data modification are done by individual users. The purpose of security, once a user is remove from the group, the blocks which were previously signed by this revoked user must be resigned by an existing system.

In this system, we purpose a novel public verify technique for the integrity of shared data with efficient user revocation in a mind. By applicability idea of proxy re-signatures. It grant the cloud to re-sign blocks on favor of existing users during the revocation, so that existing users do not need to download and re-sign blocks by themselves. In a public verify , it always able to audit the integrity of shared data without the fetching of whole data from the cloud, even if some part of shared data has been re-sign by cloud. This mechanism is able to support batch auditing by verifying multiple auditing task simultaneously. Experimental results shows that our mechanism can significantly improve the efficiency of user revocation.

Key Words: *Public auditing, shared data, user revocation, cloud computing.*

Introduction

Cloud computing is term used to describe a set of IT services that are provided to a customer over a network on a least basis and the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. This section explores some of the alternative definition for the cloud and begins by looking at the clouds key characteristics.

In a cloud computing security or, more simply, cloud security is an involving sub domain of computer security, network security and more broadly information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, application and the associated infrastructure of cloud computing. Organizations use the cloud in a variety of different service models (SAAS, PAAS, and IAAS) and deployment models (Private, Public, Hybrid, and Community). Cloud Security problems are coming from Loss of control, Lack of trust (mechanisms), Multi- tendency. Cloud Security is security principles applied to protect data, applications and infrastructure associated within the Cloud Computing technology. Cloud security is important for increasing usage of Cloud Services in non-traditional sector, growing adoption of Cloud Services in government departments, rise in Cloud Service-specific Attacks, Growing usage of Cloud Services of Critical Data Storage.

Motivation

This system can be used by multiple users. In this by improving software of secure data on the cloud for insecure data. Users can added various files in the form of text, image, audio, video etc. through the program by using encryption algorithm so that it can be stored on cloud. Thus we can secure data on a cloud. Due to this efficiency is increase and data will be secure on the cloud.

Literature survey:

Ateniese et al. proposed Provable Data Possession at Untrusted Stores, allows a public verifier to check the correctness of a clients data stored at an untrusted server. By utilizing RSA-based homomorphic authenticators and sampling strategies, the verifier is able to publicly audit the integrity of data without retrieving the entire data,

which is referred to as public verifiability or public auditing [1].

Zhu et al. proposed Dynamic Audit Services for Integrity Verification of Outsourced Storage in Clouds exploited the fragment structure to reduce the storage of signatures in their public auditing mechanism. In addition, they also used index hash tables to provide dynamic operations for users [2].

Wang et al. implemented a concept of Towards Secure and Dependable Storage Services in Cloud Computing is able to preserve users confidential data from the TPA by using random markings. In addition, to operate multiple auditing tasks from different users efficiently, they also extended their mechanism to support batch auditing [3].

B. Wang et al. proposed Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud a mechanism for public auditing shared data in the cloud for a group of users. With ring signature-based homomorphic authenticators, the TPA can verify the integrity of shared data but is not able to reveal the identity of the signer on each block [4].

Y Zhu et al. proposed efficient provable Data Profession for Hybrid Cloud in Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature schemes cannot work on the outsourced data without a local copy of data. In addition, it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large-size files. Moreover, the ability to audit the correctness of data in a cloud environment can be formidable and expensive for cloud users. Therefore, it is crucial to realize public audit-ability for CSS, so that data owners (DOs) may resort to a TPA, who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds. [5]

Peterson et al.proposed D.: Provable Data Possession at Untrusted Stores which allows a client to verify the integrity of her data stored at an untrusted server without retrieving the entire file. However, this mechanism is only suitable for static data. To improve the efficiency of verification, constructed scalable and efficient PDP using symmetric keys. [6]

Golle ET al.proposed Cryptographic primitives enforcing communication and storage complexity, the concept of enforcement of storage complexity and provided efficient schemes. Unfortunately the guarantee they provide is weaker than the one provided by PDP schemes since it only ensures that the server is storing something at least as large as the original file but not necessarily the file itself. [7]

Yu et al.proposed Efficient public integrity checking for cloud data sharing with multi-user modification, designed a dynamic public integrity auditing scheme with secure group user revocation. The scheme is based on polynomial authentication tags and adopts proxy tag update techniques, which makes their scheme support public checking and efficient user revocation. [8]

Libert et al.proposed Scalable group signatures with revocation a new scalable revocation method for group signature based on the broadcast encryption framework. However, the scheme introduces important storage overhead at group user side. And to enhance the former scheme which could obtain private key of constant size. In their scheme, the unrevoked members still do not need to update their keys at each revocation. [9]

Boyang Wang et al. did Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud 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, it allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users do not need to download and re-sign blocks by themselves[10].

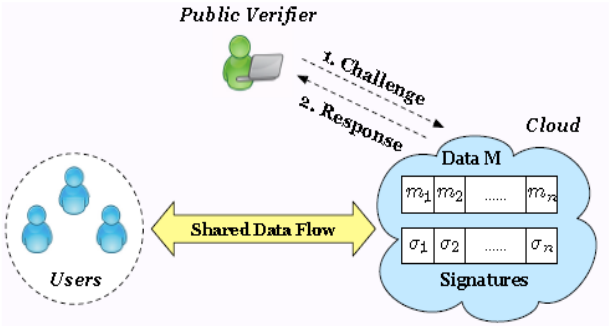
2. PROPSED SYSTEM

In this system, we propose Panda, a novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. Our proposed mechanism is scalable, which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing.
The system can be used by multiple users. In this by improving software for secure data on the cloud from unsecure data. User can add various files in the text and image through the program by using encryption algorithm so that it can be stored on cloud. Thus we can secure data on the cloud. Due to this efficiency is increase and data will be secure on the cloud.

3. SYSTEM ARCHITECTURE

The system model during this three entities: the cloud, the public supporter, and users (who share knowledge as a group). The cloud offers knowledge storage and sharing services to the cluster. The public verifier, like a consumer UN agency would love to utilize cloud data for specific functions (e.g., search, computation, data mining, etc.) or a

Third-Party Auditor (TPA) UN agency will provide verification services on knowledge integrity, aims to check the integrity of shared knowledge via a challenge and response protocol with the cloud. Within the cluster, there is one original user and a variety of cluster users. The original user is that the original owner of information. This original user creates and shares knowledge with alternative users in the group through the cloud. Each the first user and group users' square measure ready to access, transfer and modify shared knowledge. Shared knowledge is split into variety of blocks. A user within the cluster will modify a block in shared data by activity associate degree insert, delete or update operation on the block.



Each blocks in the diagram having its own work or the advantages as follows:
1) Public Verifier: The public verifier is able to correctly check the integrity of shared data. That means it checks the correctness of the shared data that is share by the user.
2) User: User is the person who shares the data in the group or as a group.
3) Cloud: This is an entity that provides data storage service.
4) Public Auditing: The public verifier can audit the integrity of shared data without retrieving the entire data from the cloud, even if some block.

4. CONCLUSIONS

Thus, we have proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, it allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Thus, the cloud can improve the efficiency of user revocation and existing users in the group can save a sign cant amount of computation and communication resources during user revocation.

ACKNOWLEDGEMENT

We would like to take this opportunity to thank our internal guide **Prof. S.R.LAHANE for** giving us all the help and guidance we needed.

REFERENCES

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

[2] 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 the Proceedings of ACM SAC 2011, 2011, pp. 15501557.

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

[4] 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. 295302.

[5] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau. Efficient provable data possession for hybrid clouds. In Proceedings of the 17th ACM conference on Computer and communications security, pages 756–758, 2010.

[6]. D. Cash, A. Kupcu, and D. Wichs, "Dynamic Proofs of Retriev-ability via Oblivious RAM," in Proceedings of EUROCRYPT 2013, 2013, pp. 279–295.

[7].Philippe Golle, Ilya Mironov. Cryptographic primitives enforcing communication and storage complexity, in Stanford University USA.

[8]. J. Yuan and S. Yu. Efficient Public Integrity Checking for Cloud Data Sharing with Multi-User Modification.

[9]. Benoit Libert, Thomas Peters, and Moti Yung. Scalable group signatures with revocation in Universities catholique de Louvain, ICTEAM Institute (Belgium) Google Inc. and Columbia University (USA).

[10].Boyang Wang, Baochun Li, and Hui Li,"Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud", IEEE TRANSACTIONS ON SERVICE COM-PUTING NO: s99 VOL:PP YEAR 2014.