ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
DIIF 0.876

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 651-654

Providing Privacy and Data Integrity in Dynamic Group Using TPA Over Cloud Computing

[1]Gaddale Jaya Bharathi , [2]Mohammed Gulzar

[1]M.Tech Research Scholar, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, India
[2]Assosiative professor, Department of CSE, Dr.K.V Subba Reddy Institute of Technology, Kurnool, India

Abstract:- 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 resignatures, 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. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved. Meanwhile, the cloud, which is not in the same trusted domain with each user, is only able to convert a signature of the revoked user into a signature of an existing user on the same block, but it cannot sign arbitrary blocks on behalf of either the revoked user or an existing user. By designing a new proxy re-signature scheme with nice properties, which traditional proxy re signatures do not have, our mechanism is always able to check the integrity of shared data without retrieving the entire data from the cloud. Here we have to focus on data transmitted with secure manner and revocation in cloud in open stack architecture with different techniques.

Keywords: Voyage Package. Public auditing, shared data, user revocation, cloud computing.

1. INTRODUCTION:

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing is one of today's most exciting technologies due to its ability to reduce costs associated with computing while increasing flexibility and scalability for computer processes[2][3]. During the past few years, cloud computing has grown from being a promising business idea to one of the fastest growing parts of the IT industry. In project the development of a technique through cloud computing in which user will handle systems from far distances with the help of centralized server and can access applications as well insert them from client machines, and can store data on data storage area on proxy server. Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally.[4] Undertaking a private cloud project requires a significant level and degree of engagement to virtualizes the business environment, and it will require the organization to reevaluate decisions about existing resources. When it is done right, it can have a positive impact on a business, but every one of the steps in the project raises security issues that must be addressed in order to avoid serious vulnerabilities. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept" In this project SAAS service is being used.

2. LITERATURE SURVEY

[9]To introduce the TPA effective safely, the audit process should not compensate an additional fee for online users and carry-in; there is no new compromise to the privacy of user data. This proposed approach is a secure cloud storage mechanism as public auditing mechanism for secure cloud storage. At the same time this approach extends to the TPA performance to audit multiple users efficiently. By showing high efficiency and provable security and performance analysis a wide range of security, the proposed scheme.

[6]They have utilized the idea of proxy re-signatures to allow the cloud to re-sign blocks on behalf of existing users during user revocation, so that existing users need not to download and re-sign blocks by themselves. Moreover, this mechanism is able to support batch auditing by verifying multiple auditing tasks simultaneously. Experimental results show that the mechanism

can significantly improve the efficiency of user revocation.

[12] They have exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With this mechanism, the identity of the signer on each block in shared data is kept private from a third party auditor (TPA), who is still able to publicly verify the integrity of shared data without retrieving the entire file.

[5] This system proved the data freshness (proved the cloud possesses the latest version of shared data) while still preserving identity privacy. An experimental result of this ensures that retrieved data always reflects the most recent updates and prevents rollback attacks.

[3] The main problem associated with [12] is the size of signatures and verification time linearly increase with the number of users in the group that is solved with Knox considering audit of the data integrity which is to be shared with a large group while still preserving identity privacy from the TPA by leveraging group signatures.

III. PROBLEM STATEMENT

Current working scenario involves paper based work for Data analysis and verification. Data Storage is one way to mitigate the privacy concern. Unauthorized users can leak or misuse the data, this problem still remains due to the paper based work. This features of cloud computing evolved various concerns related to user's identity, data integrity and users availability. Ultimately this influences to propose an enhanced model in order to audit the data integrity and keeping the identity privacy with efficient user revocation while sharing.

IV. SYSTEM OVERVIEW

A. Existing System

To protect the integrity of data in the 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 all the signatures. One of the most significant and common features of these mechanisms is to allow a public verifier to efficiently check data integrity in the cloud without downloading the entire data, referred to as public auditing (or denoted as Provable Data Possession).This public verifier could be a client who would like to utilize cloud data for particular purposes (e.g., search, computation, data mining, etc.) or a third party auditor (TPA) who is able to provide verification services on data integrity to users. Most of the previous works focus on auditing the integrity of personal data. An existing system the file uploaded in cloud which not signed by user in each time of upload. So that integrity of shared data is not possible in existing system. However, since the cloud is not in the same trusted domain with each user in the group, outsourcing every user's private key to the cloud would introduce significant security issue [5]. Especially when the number of re-signed blocks is quite large. Existing users may access their data sharing services provided by the cloud with resource limited devices, such as mobile phones

Disadvantages

- 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.
- No data privacy
- No identity privacy

V. PROPOSED SYSTEM

Examining the above research work we have proposed a new method through which we not only audit the data integrity but also conserve identity privacy with user revocation. Our proposed mechanism should posses the following Properties:

1) Correctness: The TPA should be correctly check the Integrity of shared data correctly.

2) Efficient User Revocation: When a user is revoked from the group, the blocks signed by that user can be re-signed efficiently. As well as, only existing members in the group can only generate valid signatures on shared data and the members which are revoked from the group cannot compute the valid signatures on shared data.

3)Public Auditing: The Third Party Auditor the integrity of shared data can be audit by Third Party Auditor without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud. For achieving these properties we are going to use some predefined cryptographic primitives.

Proxy re-signatures A Semi-trusted proxy acts as a translator of signatures between two users first proposed by Blaze et al. [10], More Briefly, the proxy converts a signature of one user into a signature of other user on the same block. Without knowing any private keys of the two users, which means that it cannot sign any block on behalf of any user. In this paper, we have improved the efficiency of user revocation, by acting cloud as a proxy and convert those signatures during user revocation.

ISSN (Online): 2349-7084

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 2, ISSUE 9, SEPTEMBER 2015, PP 651-654

Ring Signatures The ring signatures concept is first proposed by Rivest et al. [4] in 2001. With ring signatures, a verifier is convinced that a signature is computed using one of group member's private keys, but the verifier is not able to determine which one. This property can be used to preserve the identity of the signer from a verifier. We have reviewed that the following algorithms will help us to construct our proposed mechanism.

KeyGen: In KeyGen each user in the group generates her public key and private key.

ReKey: For each pair of user in the group , cloud computes a resigning key with ReKey.

ProofGen: Proof of possession of shared data is generated.

Proof Verify: In Proof Verify TPA verifies the correctness of proof responded by cloud.

ReSign: In ReSign algorithm signature of revoked user is converted to the original user.

RingSign: In a RingSign a user in the group signs a block with their private key & all group members public key.

RingVerify: In this verifier is allowed to check whether the given block is signed by that the group member only.

Homomorphic verifiable tags: These are the basic tools to construct data auditing mechanisms. Besides user with a private key which generates the valid signatures, a homomorphic authenticable signature scheme denotes a homomorphic authenticator based on signatures, which also satisfies the Blockless verification and Non-malleability. Discussing in details to our auditing mechanism.

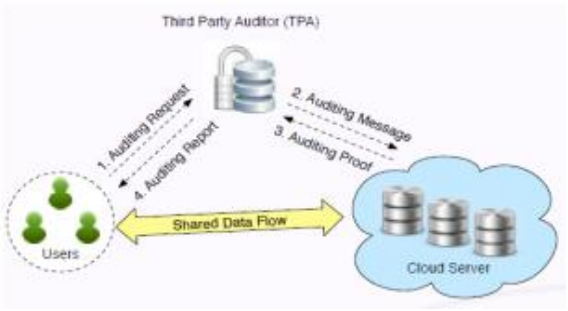

Fig 1. System Model

Advantages

- Support batch auditing
- It can perform multiple auditing tasks simultaneously
- Improve the efficiency of verification for multiple auditing tasks
- Preserve data privacy from public verifiers
- Leverage index hash tables from a previous public auditing solution to support dynamic data.

A user (original user or a group user) who wants to verify the integrity of shared data first sends an auditing request to the TPA. On receiving that auditing request, TPA sends an auditing message to the cloud server, and gets an audit proof of shared data from the cloud server. Then the TPA confirms the correctness of the auditing proof. Eventually, the TPA conveys an auditing report to the user based on that result of the verification.

It includes with nine algorithms: **KeyGen, SigGen, Modify ReKey, ReSign, RingVerify, RingSign, ProofGen and ProofVerify.** In **KeyGen**, users generate their own public/private key pairs. In **ReKey**, the cloud computes a resigning key for each pair of users in the group. He/she computes a signature on each block as in Sign. After that, if a user in the group modifies a block in shared data, the signature on the modified block is also computed as in Sign. In **ReSign**, a user is revoked from the group, and the cloud re-signs the blocks, which were previously signed by this revoked user, with a resigning key. In **SigGen**, a user (either the original user or a group user) is able to compute ring signatures on blocks in shared data. Each user in the group is able to perform an insert, delete or update operation on a block, and compute the new ring signature on this new block in Modify. The verification on data integrity is performed via a challenge-and-response protocol between the cloud and a public verifier. More specifically, the cloud is able to generate a proof of possession of shared data in **ProofGen** under the challenge of a public verifier. In **ProofVerify**, the TPA verifies the proof and sends an auditing report to the user. Before the original user outsources shared data to the cloud, she decides all the group members, and computes all the initial ring signatures of all the blocks in shared data with her private key and all the group members' public keys. After shared data is stored in the cloud, when a group member modifies a block in shared data, this group member also needs to compute a new ring signature on the modified block. In **ProofVerify**, a public verifier is able to check the correctness of a proof responded by the cloud. In **ReSign**, without loss of generality, we assume that the cloud always converts signatures of a revoked user into signatures of the original user. The reason is that the original user acts as the group manager, and we assume he/she is secure in our mechanism. Another way to decide which re-signing key should be used when a user is revoked from the group is to ask the original user to create a priority list (PL). Every existing user's id is in the PL and listed in the order of resigning priority. When the cloud needs to decide which existing user the signatures should be converted into, the first user shown in

the PL is selected. To ensure the correctness of the PL, it should be signed with the private key of the original user (i.e., the group manager).

VI. CONCLUSION AND FUTURE WORK

Now a day's IT Infrastructure is propelling towards cloud computing, but the data integrity concerns with identity privacy which must be addressed. In this paper, we reviewed various privacy preserving mechanisms for static group in cloud computing and propose a new idea for identity privacy with efficient user revocation in cloud computing environment. We have furnished the simulated implementation of HAPS [6] and HARS [12] algorithms. Presently this research is under development to find the system for preserving identity privacy for revocation of the user or group member while sharing the data on cloud. In future work we would be focusing on developing a complete framework that would cover all integrity aspects related to data with identity privacy for dynamic group. We thought this channelized project would lean to aid the institutions/organizations to encourage towards the Cloud environment and construct rich IT infrastructure.

REFERENCES

[1] John W. Rittinghouse James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press Taylor & Francis Group 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742 © 2010 by Taylor and Francis Group, LLC CRC Press is an imprint of Taylor & Francis Group, an Informa business.

[2] 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. 598–610.

[3] B. Wang, B. Li and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", ACNS2012

[4] 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.

[5] P. Maheswari, B. Sindhumathi "AFS: Privacy Preserving Public Auditing With Data Freshness in the Cloud" IOSR Journal of Computer Engineering (IOSRJCE) PP 56-63

[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

[11]Zahir Tari, RMIT University, "Security and Privacy In Cloud Computing", IEEE Cloud Computing Published by the IEEE Computer Society 2014

[12]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

[13]Zhifeng Xiao and Yang Xiao, Senior Member, IEEE, "Security and Privacy in Cloud Computing", IEEE Communications Surveys & Tutorials, vol. 15, no. 2,Second quarter 2013.

[14]C. Wang, Q. Wang, K. Ren, and W. Lou, "PrivacyPreserving Public Auditing for Data Storage Security in Cloud Computing," in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533

BIOGRAPHIES

G.Jaya Bharathi,M.Tech Research Scholar, Department of CSE, Dr.K.V.Subba Reddy Institute of Technology, Kurnool, India. G.Jayabharathi, I am Doing project in M.tech research on domain cloud computing and the topic is **"Providing Privacy and Data Integrity in Dynamic Group Using TPA Over Cloud Computing".**

Mohammed Gulzar C. received his B.E degree in CSE from VTU,Belgaum in 2004, the M.TECH. Degree in CSE from VTU, Belgaum, in 2008. Currently he is working as an Associate Professor in Dr. K.V Subbareddy institute of Technology, Kurnool, Andhra Pradesh, India. He has nine years of experience in teaching.