www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21424-21427
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.39

A Formation of Cloud Data Sharing With Integrity and User Revocation

Prof. Butkar U D [1] ***,Ms. Sasane Minal*** [2] ***, Ms. Sonali Salpure*** [3]
Assistant Professor [1]
BE Student [2]
BE Student [3]

Abstract:
Cloud computing and storage services, data is not only stored in the cloud, but routinely shared among a large number of users in a group. It remains elusive, however, to design an efficient mechanism to audit the integrity of such shared data, while still preserving identity privacy. In this paper, we propose Knox, a privacy-preserving auditing mechanism for data stored in the cloud and shared among a large number of users in a group. In particular, we utilize group signatures to construct homomorphic authenticators, so that a third party auditor (TPA) is able to verify the integrity of shared data for users without retrieving the entire data. Meanwhile, the identity of the signer on each block in shared data is kept private from the TPA. With Knox, the amount of information used for verification, as well as the time it takes to audit with it, are not affected by the number of users in the group. In addition,Knox exploits homomorphic MACs to reduce the space used to store such verification information. Our experimental results show that Knox is able to efficiently audit the correctness of data, shared among a large number of users.
Keywords**-**voting system, group signature, Shared Data, Cloud Computing, vector commitment, Third party Auditor

Introduction:

The improvements and enhancements in cloud computing motivates enterprises and also organizations to outsource their data to third party cloud service providers (CSP's) which will result in improvements in the data storage limitation of resource constrain local devices. In market, already some cloud storage services are available like simple storage service (S3) online data backup services of Amazon and software like Google Drive, Drop box, Mozy, Bitcasa and Memopal built for cloud application. In some cases cloud server sometime returns invalid results such as hardware/software failure, malicious attack and human maintenance. Security and privacy of cloud user's data should be protected by data integrity and accessibility. To overcome the security issues of today's cloud storage services, simple replication and protocols like Rabin's data dispersion scheme are not sufficient for practical application. For achieving the integrity and availability of remote cloud storage, some various solutions and their different variants have been proposed. In these solutions, when a scheme supports modification of data, it is known as dynamic scheme, otherwise static one. A scheme is publicly verifiable that means the integrity check of data can be performed not only by data owners, but also by the third party auditor (TPA). However, the focus of the dynamic scheme is on the cases where only and only data owner could modify the data of cloud. Recently, the development of cloud computing emerged some applications where the services of cloud can be used as a collaboration platform. In these software development environments, one or more than one (multiple) users in a group need to share source code as well as they needs to access, compile, modify and run the source code share by user at any time. The new model of cooperation network in cloud provides the infeasibility of data for auditing the remote data, where only the data owner can update its data. It will result in terrific communication and computation to the data owner which causes the single point of data owner. To achieve multiple data operation, Wang et al. put forth data integrity based on ring signature. In the scheme, it does not consider the user revocation problem and the cost of auditing is linear to the data size and group size. To further raise up the previous scheme and support group user revocation, Wang et al. proposed a scheme based on proxy re-signatures. However, this scheme assumes that authenticated and private channels exist between the pair

of entities and there is no collusion among them. Also, cost of auditing the scheme is linear to the size of the group. Another attempt to improve the previous scheme and make the scheme scalable, efficient and collusion resistant, Yuan and Yu designed a dynamic public integrity auditing scheme with group user revocation. However, in their scheme, the authors do not consider the secrecy of data among the group users. That means, their scheme could efficiently support plain text of data update and integrity auditing, while not ciphertext data. In their scheme, if data owner shares group key among the users of group, revocation of any group user allow the group users to update their shared
key. Also, the owner of the data does not take part in the user revocation phase, where the user revocation phase is itself conducted by the cloud. In this case, the malicious cloud server will result in collusion of revoked user and the cloud server where the cloud server could update data number of times as designed and provide a legal data finally. Due to above mentioned deficiency; we propose a construction which includes data encryption and decryption during the data modification processing, secure and efficient user revocation and also removal of redundant data. Here, vector commitment scheme will be applied over the database. Then we apply the Asymmetric Group Key Agreement
(AGKA) to support ciphertext database update among group users and we also use group signatures for efficient group user revocation. The user in the group will be able to encrypt or decrypt a message from any other group users when the group users use the AGKA protocol to encrypt or decrypt the share database. The collusion of the cloud and revoked group users will be prevented by the group signature. Each file uploaded to the cloud is also requires a set of privileges to specify which kind of users can access the files and which users is allowed to perform the duplicate check and. Before submitting this duplicate check request for some file, the user needs to take his own privileges and also files as inputs. The user is able to find a duplicate for this file if and only if there is a copy of this file and matched privileges stored in cloud. For example, in a company, many different privileges will be assigned to the employees. The data will be moved to the storage server provider (SCSP) in the public cloud with specified privileges and the de-duplication technique will be applied to store only one copy of the same file in order to save cost and efficient management. Because of privacy consideration, some files will be encrypted and will also be allowed the duplicate check by employees with specified privileges to realize the access control. Traditional de-duplication systems based on convergent encryption, although providing confidentiality to some extent, do not support the duplicate check with differential privileges. In other words, in the de duplication based on convergent encryption technique no differential privileges have been considered. If we want to realize both de- duplication and differential authorization duplicate check at the same time, it seems to be contradicted.

Existing System:
Considering data security, a customary approach to guarantee it is to depend on the server to
implement the entrance control after verification, which implies any unforeseen benefit heightening will uncover all data. In a mutual occupancy cloud computing environment, things turn out to be far more terrible. Data from diverse customers can be facilitated on discrete virtual machines (VMs) however live on a solitary physical machine. Data in an objective VM could be stolen by instantiating another VM co-occupant with the objective one. As to of documents, there are a progression of cryptographic plans which go similarly as permitting an outsider inspector to check the accessibility of records for the benefit of the data provider without spilling anything about the data, or without bargaining the data provider's secrecy. Similarly, cloud clients presumably won't hold the solid conviction that the cloud server is benefiting work regarding classification. A cryptographic arrangement, with demonstrated security depended on number-theoretic presumptions is more alluring, at whatever point the client is not superbly content with believing the security of the VM or the genuineness of the specialized staff. These clients are roused to encrypt their data with their own particular keys before transferring them to the server. But there are several disadvantages in the existing system:-

1. Unexpected privilege escalation will expose all
2. It is not efficient.
3. Shared data will not be secure.

PROPOSED SYSTEM
In this paper, we study the problem of Public Authentication Inspection for Shared Dynamic Cloud Data with Group User Revocation Including Backup And Data Storage Our contributions are:
For cipher text database, we explore on the efficient and secure shared data integrity

auditing for multi-user operation. We intend an efficient data auditing scheme along with new features such as countability by incorporating the vector commitment primitives, traceability, asymmetric group key agreement and group signature. The analysis results show that our scheme is secure and efficient as we provide the efficiency and security analysis of our scheme which will result in back-up and data storage in cloud.
The authorized duplicate check in the hybrid cloud architecture is supported by several de duplication constructions and this authorized duplicate check scheme comparatively incurs minimum overhead than normal operations.
The below diagram shows cloud storage model which has been referred from "Public integrity auditing for shared dynamic cloud data with group user revocation,"

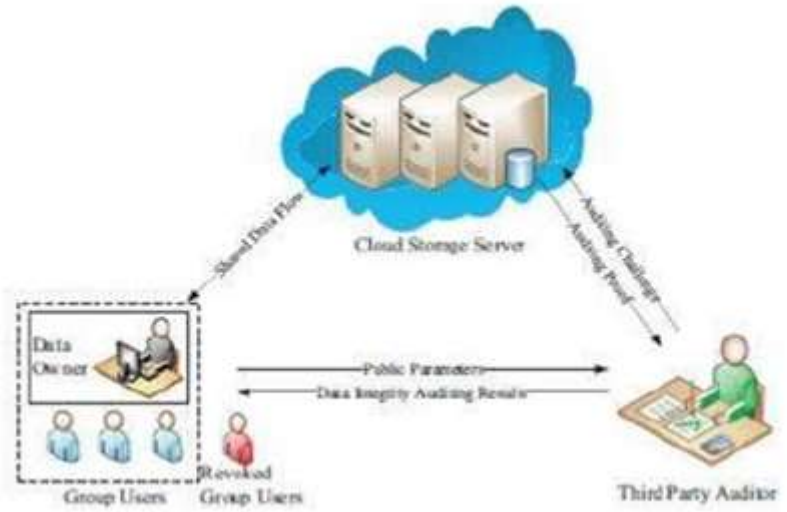

Fig. System Architecture

System Modules:

1.User Module
2.Auditor Module
3.Admin Module

User Module:

- User module is responsible for following operations.
- Registration: This module is responsible for user registration with details for using system. Only those users can login into cloud server who is registered user.
- File Upload: User uploads file with blocks along with performing encryption using secrete key.
- Download: In this module user can download the le and can decrypt data using his secret key.
- Re-upload: Once user re-sign the blocks of le then this module allow user to re-upload the downloaded les.
- Unblock: This module provide some questions and by answering these security user account will be unlocked.

Auditor Module:

- Verification of Files: The public verier is responsible for checking the scalability of shared data.
- Files View: This module allow auditor to view the all details of le upload, le download, blocked user, re-upload.

Admin Module:

- View Files: This module allow auditor to view the all details of le organization.
- Block User: Admin have authority to block the misbehave user account.

Application:

In this section, we briefly discuss the applicability of our proposed scheme in real-world application scenarios. In particular, we consider two contrasting applications. with group size and data size. Recently, Wang et al. enhanced their previous public integrity verification scheme with the support of user revocation. Nevertheless, their design assume

that there is non-collusion among cloud servers and revoked users. However, once cloud servers and the revoked users work together during their proxy tag update process, they can discover the secret keys of all other valid users. What is more, verification cost of the TPA (can also be users) in ref. is linear to the size of group. Batch verification is not supported in their design. Therefore, this scheme is limited in its scalability.

Advantages:

1. Security: It should check the user authenticity by password to verify user identity. By using digital signature it should satisfy privacy certifications.
2. Efficiency: The efficiency for the any data computation as well as storage data issue can facilitated by
3. any group user which is depend on the size of the shared data.
4. Accountability: According to improper storage server of the cloud tampered with database.
5. Traceability: In this the generation algorithm generates the data and the valid group signature, the data owner trace the last user who update the shared data.

Correctness: Data updated by valid group user which is supports to encrypted database by correct result.

FUTURE ENHANCEMENTS

This paper presents a novel approach to securing personal and business data in the Cloud. This approach introduce a security at the time of upload process itself because to avoid the unwanted uploads in the user account. In the future more security will be provided by change the security settings frequently and based on the unauthorized access.

CONCLUSION

In this the database with efficient and secure updates is way to solve the problem of verifiable data storage. We implement a scheme to realize secure and efficient auditing of data for share dynamic data with multiuser modification. In this paper, the Victor commitment algorithm helps for sharing data within the group on cloud in efficient way. Asymmetric key generation algorithm and barcode scheme adds on the security by storing the in encrypted form. The scheme vector commitment, Asymmetric Group Key Agreement.

REFERENCES

[1] T. Jiang, X. Chen, and J. Ma, “Public integrity auditing for shared dynamic cloud data With group user revocation,” in Proc. Of IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015

[2]Amazon. (2007) Amazon simple storage service (amazon s3).Amazon. [Online]. Available: http://aws.amazon.com/s3/

[3] Google. (2005) Google drive. Google. [Online]. Available:http://drive.google.com/

[4] Dropbox. (2007) A file-storage and sharing service. Dropbox.[Online].Available: ttp://www.dropbox.com/

[5] Mozy. (2007) An online, data, and computer backup software.EMC. [Online]. Available:http://www.dropbox.com/

[6] Bitcasa. (2011) Inifinite storage. Bitcasa. [Online]. Available:http://www.bitcasa.com/

[7] Memopal. (2007) Online backup. Memopal. [Online].Available: http://www.memopal.com/

[8] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, ” Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud” in Proc. Of IEEE Cloud 2012, Hawaii, USA, Jun. 2012, pp. 295–302.

[9] D. Catalano and D. Fiore, “Vector commitments and their applications,” in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.

[10] B. Wang, L. Baochun, and L. Hui, “Public auditing for shared data with efficient user revocation in the cloud,” in Proc. Of IEEE INFOCOM 2013, Turin, Italy, Apr. 2013, pp. 2904–2912

[11] Q. Wu, Y. Mu, W. Susilo, B. Qin, and J. Domingo-Ferrer,“Asymmetric group key agreement,” in Proc. of EUROCRYPT 2009, Cologne, Germany, Apr. 2009, pp. 153–170.

[12] J. Yuan and S. Yu, “Efficient public integrity checking for cloud data sharing with multi-user modification,” in Proc. of IEEE INFOCOM 2014, Toronto, Canada, Apr. 2014, pp. 2121– 2129.

[13] D. Boneh and H. Shacham, “Group signatures with verifier local revocation,” in Proc. of ACM CCS, DC, USA, Oct. 2004, pp. 168–177.