Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

SURVEY ON DYNAMIC DATA SHARING IN PUBLIC CLOUD USING MULTI-AUTHORITY SYSTEM

Priyanka Phasale .
Department of Computer Engineering,
Vishwabharati Academy's College of Engineering, Ahmednagar, India

Priyanka Kokate
. Department of Computer Engineering,
Vishwabharati Academy's College of Engineering, Ahmednagar, India

Prof M.C. Kshirsagar
Department of Computer Engineering,
Vishwabharati Academy's College of Engineering, Ahmednagar, India

ABSTRACT
The continuous development of cloud computing, several trends are opening up to new forms of outsourcing. Public data integrity auditing is not secure and efficient for shared dynamic data. In existing scheme figure out the collusion attack and provide an efficient public integrity auditing scheme, with the help of secure group user revocation based on vector commitment and verifier–local revocation group signature. It provides secure and efficient scheme which support public checking and efficient user revocation. Problem of existing work they used TPA (Third party auditor) for key generation and key agreement. Use of TPA as central system if it fails then whole system gets failed. If we are working with cloud, user identity is major concern because user doesn't want to reveal his personal information to public. This concept not included in it. In this paper, based these con's we proposed a dynamic data sharing in public cloud using multi-authority system. The proposed scheme is able to protect user's privacy against each single authority.

KEYWORDS: Public integrity auditing, CSP, TPA, dynamic data, VC, ASGA.

INTRODUCTION
Cloud computing refers application and services that run on distributed networks. Cloud storage is important service of cloud computing which allow data owners to move data from their local computing system to the cloud. Therefore in any infrastructure data loss or discard not been accessed. Sometime CSP (cloud service provider) might be dishonest that's why owners need to ensure that data are stored in cloud or not [1][2]. Recently some research considers several remote integrity checking protocols which allow the auditor to check the data integrity on remote server [2]. In [1], X-Chen proposed secure and efficient public data integrity auditing for shared dynamic data. Overcome collusion attack of cloud storage server against security. To protect security and privacy of cloud user's data [1]

LITERATURE REVIEW:
In the literature review topical method over the cloud data approaches as discuss, below in literature some of them are discussed:

1) Tao Jiang, Xiao Feng Chen, and Jian Feng Ma: Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation, IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015
This paper represent secure and efficient public data integrity auditing for sharing dynamic data against the collusion attack, Provide secure group user revocation base on VC(Vector Commitment) and VLR(Verifier-local revocation)group signature. Organizations outsource own data to third party CSP(Cloud Service providers).contribution of these scheme: Propose efficient data auditing scheme by using VC and AGKA (Asymmetric group key agreement),GS(Group signature)to support ciphertext group user revocation and encrypt/decrypt share database. CSM (Cloud storage model) indicate three entities:

1. CSS (Cloud storage server): share privilege to access and modify number of group users.
2. GU (Group user) who are authorized to access and modify the data by the data owner.
3. TPA: any entity which able to conduct data integrity of share data storage in cloud server.

2) Madhuri R. Rokade et al, "Providing Data Utility on Cloud using Slicing approach and Dynamic Auditing Protocol using Third Party Auditor to maintain Integrity of Data" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 852-855.

A method presents a new approach called slicing to privacy-preserving data. Slicing overcomes the limitations of generalization and bucketization and preserves better utility while protecting against privacy threats in cloud. That proposed an efficient and inherently secure dynamic auditing protocol which audits the data present in the cloud periodically and also whenever auditor wants to check it. Also dynamic data changes are also audited. Furthermore, auditing scheme incurs less communication cost and less computation cost of the auditor by moving the computing loads of auditing from the auditor to the server, which greatly improves the auditing performance and can be applied to large-scale cloud storage systems.

3) C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp no. 525533.

Motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content. This scheme is the first to support scalable and efficient privacy preserving public storage auditing in cloud. Scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. TPA would not 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 reduce the user's fear of their outsourced data leakage. TPA may concurrently handle multiple audit sessions from different users for their outsourced data files; we further extend our privacy preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

4) 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.

The author designed dynamic public integrity auditing scheme with group user revocation. Yuan and yu not consider data secrecy of group users in their scheme that means scheme efficiently support plaintext data update and integrity auditing not cipher text data. Design polynomial authentication tag and adopt proxy tag update technique. If data owner share group key with group users and defection or revocation occur any group user will force to other group user to update their shared key. Sometime data owner not take part in user revocation phase, where many time cloud server update the data and provide data legally last.

5) B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. of IEEE CLOUD 2012, Hawaii, USA, Jun. 2012, pp. 295–302.

Oruta consider how to audit the integrity of shared data in cloud with static group. Group is predefined before shared data created in cloud. Membership of users is constant in the group. Original user decides who is able to share data to the cloud before outsourcing. Problem in these schemes is how to audit the integrity of shared data in cloud with dynamic group. New user added onto group but existing user can be revoked during data sharing.

6) D. Catalano and D. Fiore, "Vector commitments and their applications," in Public-Key Cryptography - PKC 2013, Nara, Japan, Mar. 2013, pp. 55–72.

This paper introduce new simple and powerful commitment mechanism should not allow a sender to change mind about committed message. VC Scheme is collection of six-polynomial time algorithm (Vc.KeyGen, Vc.Com, Vc.Open, Vc.Ver, Vc.Update, and Vc.ProofUpdate). Vc allows to commit ordered sequence of q value (m1……mg) to single message Vc require position binding to satisfaction means two different value at the same position. Vc require hiding updatable property, Use two algorithm to update the commitment and opening message. First algorithm allows committer who created commitment and want to update changing message. Second algorithm allows holders of an opening of message to update their proof.

PROPOSED WORK:

Problems of Existing Work:

1. As in base paper [1], Used TPA (Third party auditor) for key generation and for key agreement.
2. TPA (Third party auditor) is central system, if it fails then whole system get failed.

3. If we are working with cloud, user identity is major concern user doesn't want to reveal his personal information to public. This concept not included in it.

So based on these cons, we proposed a Dynamic Data Sharing in Public Cloud using Multi-Authority System

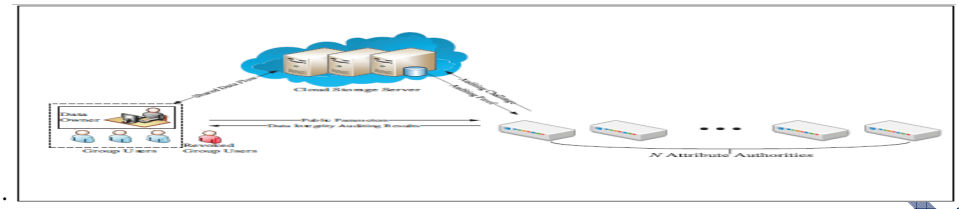

Fig 1: Proposed system

The proposed schemes are able to protect user's privacy against each single authority. Authorities are assumed to have powerful computation abilities, and they are supervised by government offices because some attributes partially contain users' personally identifiable information. The whole attribute set is divided into N disjoint sets and controlled by each authority, therefore each authority is aware of only part of attributes.

We have assumed semi-honest authorities and we assumed that they will not collude with each other. This is a necessary assumption because each authority is in charge of a subset of the whole attributes set, and for the attributes that it is in charge of; it knows the exact information of the key requester. If the information from all authorities is gathered altogether, the complete attribute set of the key requester is recovered and thus his identity is disclosed to the authorities. In this sense, system is semi-anonymous since partial identity information (represented as some attributes) is disclosed to each authority, but we can achieve a full-anonymity and also allow the collusion of the authorities.

CONCLUSION

We provide security analysis of our scheme, and it shows that our scheme provide data confidentiality for group users, and it is also secure against the collusion attack from the cloud storage server and revoked group users. We provide security analysis of our scheme with a semi-anonymous attribute-based privilege control scheme to address the user privacy problem in a cloud storage server. The scheme vector commitment, Asymmetric Group Key Agreement (AGKA) and group signatures with user revocation are adopt to achieve the data integrity auditing of remote data using multiple authorities in the cloud computing system, our proposed schemes achieve not only fine-grained privilege control but also identity anonymity while conducting privilege control based on users' identity information.

REFERENCES

[1] Tao Jiang, Xiao Feng Chen, and Jian Feng Ma: "Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation", IEEE TRANSACTIONS ON COMPUTERS VOL: PP NO: 99 YEAR 2015.

[2] Madhuri R. Rokade et al, "Providing Data Utility on Cloud using Slicing approach and Dynamic Auditing Protocol using Third Party Auditor to maintain Integrity of Data",(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 852-855.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing,", in Proc. of IEEE INFOCOM 2010, CA, USA, Mar. 2010, pp no. 525533.

[4] 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.

[5] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in Proc. of IEEE CLOUD 2012, Hawaii, USA, Jun. 2012, pp. 295–302.

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