International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || Volume 3 Issue 11 || November 2014 || PP.06-09

Preserving Privacy Policy- Preserving public auditing for data in the cloud

Krishna Kumar L[1], Deepa P Sivan [2]
[1](Professor, Department of Computer science, Nehru Institute of Technology/ Anna University, India)
[2](Scholar, Department of Computer science, Nehru Institute of Technology/ Anna University, India)

ABSTRACT : Cloud computing is widely developed technology, remotely to be temporarily shared across multiple users in flexible manner than products. Users can continuously access service from the remote locations. So cloud creates issues in data security, privacy integrity, and dynamic updates. The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. In user side every time it is not possible to check data consistency of stored data on cloud storage. This problem is solving by public auditing method, which ensure integrity and to reduce online burden on cloud data storage. So user may resort to third-party auditor (TPA) to audit the data by using ring signatures. The privacy preserving identity of the signer on each block from the TPA means, the group is pre-defined before shared data is created in the cloud .The membership of each users in the group is not changed during the data sharing stage. The original user is responsible for who is able to share her data before outsourcing data to the cloud. TPA audits the integrity of shared data on cloud with dynamic group of user. In this method cloud storage service provide data sharing preserving identity privacy.

KEYWORDS : *cloud computing, privacy-preserving, public auditing, ring signature, shared data*.

I. INTRODUCTION

Cloud computing is an internet based computing which enables sharing of services. Cloud computing allows users to use applications without installation any application and access their personal file and application at any computer with internet or intranet access. Cloud applications are e-mail, e-commerce, web conferencing-shopping, customer relationship management (CRM) etc. Cloud computing is widely developed technology used in IT industries to provide services like resources, rapid resource elasticity, network access control and platform as per user require. In cloud computing the user data is centralized to the cloud. The user can access the cloud services within the help of mobile devices and internet connection. Cloud storage is a online storage in which the data store in format of file or block pattern .Cloud data stored in virtualized pools of storage that are generally given by the Third Party Auditor(TPA). The cloud provides its application, software and data services are in remotely and temporarily, user can access it's by using personal computers, mobile phones or other internet access devices. In IT industries, individuals storing their data into the cloud in flexible manner having some benefits like relief from Hardware, software, online burden of data storage, reduce the cost of capital expenditure on personal maintenance. Cloud containing majority problems are related to data sharing resources between multi-owners and group membership changes. There are many methods are using for overcome from these issues as ring signature and encryption techniques.

Today everyone depending network to developing their knowledge in any area at any time so many users from remote locations use network services continuously so there may arise some issues. The cloud containing main issues are depending privacy, security, data integrity, dynamic updates. This problem is addressed and solving by using public auditing for secure cloud. The third party auditor (TPA), who has capabilities and expertise that can periodically check the integrity of the data, which is stored in the cloud. The users cannot have the auditing capabilities than TPA. The TPA check the correctness of data stored in cloud on behalf of user and maintain the data integrity. Enabling public auditing service will play an important role for privacy data security & minimizing the data risk from misuses. The TPA is act as an external party .Which can also view the data stored in cloud and does not give the guarantee of data privacy. The auditing data in cloud can access the original data owner at any time.The cloud computing architecture contains a Third Party Auditor (TPA) for auditing the system which is connected with the particular group of the cloud storage. Group member or user is Cloud users where they store their private data into the cloud sever and also share that data with other user of Cloud system as a group member. Cloud is a system operated by the Cloud service provider, which allow to store and share data of cloud user in a system and also access service on a demand basis as pay. The cloud contains two types of storage, private and public type.

In the public anyone can access and anyone can change the cloud containing data and in the private the particular user can only access the data and the user cannot change the data without the owner's permission.

II. LITERATURE SURVEY

A View of Cloud Computing : M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia are a term of persons presented data security is one of the most important objections in the cloud computing. There is also analysis about storage area as hard disk, virtual machine memory contents and its requirements for audit-ability. Namely user-level encryption of storage is common for high-value data outside the cloud architecture, its tools and existing user information are available. This cloud approach was successfully used by TC3, in the area of healthcare company. This is used for access of data about patient records and claims, when moving their compliant application to AWS. Audit-ability could be added as an additional layer within the virtualized guest OS, and its audit-ability and confidence providing facilities to improve more security into the applications development and centralizing. Theses software responsibilities related into a single logical layer to focusing the applications and services.

B. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing : C.Wang, Q. Wang, K. Ren, and W. Lou are presented a cloud based storage system containing storage server's collections. TPA is a separate system which contains serious eight causes concerns over data confidentiality in data. Generally encryption method is used for data protection but also limit the functionality of the storage system because a few operations are supported over encrypted data storing. The challenges of secure storage system is support multiple functions with no central authority and distributed type. They propose a secure storage distributed system which propose a threshold proxy re-encryption scheme to integrate decentralized code. The distributed storage supports secure, retrieval and robust type of data storage. In the retrieval supporting secure storage distributed system a user can forward any type of data into storage servers and other user cannot able to retrieving the data recovery. The main technical contribution is proxy re-encryption scheme, which supports encrypted type messages to perform encoding. They suggest suitable parameters for the number of dispatched message copies to storage servers and the storage servers are queried by using a key server.

C. Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing : S. Yu, C. Wang, K. Ren and W. Lou are presented new challenges for data security and access control. When confidential user data sharing on un-trusted cloud server. The cryptographic methods are using for existing solutions in the disclosing data decryption keys. The problem are depends upon some of its properties fine-graininess, scalability, and confidentiality and access control are remain unresolved. In this paper mention this open challenging issue by hand, define and enforcing access policies based on data attributes, The elevate data owner to commutated this tasks ,which involved in fine-grained data access control in to un-trusted cloud servers .The main goal by exploiting and unique wise combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. They proposed scheme has salient user access properties of confidentiality and accountability.

D. Scalable and Efficient Provable Data Possession : G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik are developed a design a scalable and effective cloud based distributed storage. The design based on step by step cooperative PDP scheme, which contain light-weight and secure provably property. Using in architecture to develop a hierarchy structure which supports file storage representation. The hierarchical structure represents relationships among all blocks in the stored resources. Homomorphic verifiable is the CPDP key technique which reduces the communication bandwidth and support dynamic type operations.. The PDP or PoR is a probabilistic proof technique, which focus in the single data storage un-trusted cloud servers but not suitable for a multi cloud environment. The data possession without downloading data at un-trusted stores, not suitable for distributed cloud storage since they were not originally constructed on interactive proof system. The homomorphic doesn't responses from multiple clouds, when using a scalable and unsuitable third party auditor for verification.

E. Ensuring Data Storage Security in Cloud Computing : C. Wang, Q. Wang, K. Ren, and W. Lou are proposed distributed architecture to ensure the data correctness of IT Enterprise and users. The distributed storage system provides guarantee in redundancy and dependability. In the centralized large data centers which act as a application software as well as databases to management and services provider in the data storage server. In this work studies about ensuring the integrity of data storage containing the problem in cloud Computing. In particular, a third party auditor (TPA), to verify dynamic data and its integrity in the cloud. The dynamics data support in the forms of data operation such modification, insertion, and deletion. So the cloud data services are not limited to archive or data backup.

F. Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud : Boyang Wang, Baochun Liand Hui Li are presented on cloud and its storage services. The effective design mechanism to audit shared data integrity to preserving privacy of user identity. In particular, using a signature homomorphic authenticator. The administrators or group managers can control the group by using private key. A third party auditor (TPA) is able to verify shared data. The signer on each block identity in shared data is kept private from the TPA. Here using Knox exploits homomorphic MACs to reduce storage space to perform information verification. This is efficiently audit the data correctness and data shared among a multiple users.

G. Aggregate and Verifiably Encrypted Signatures from Bilinear Maps : D. Boneh, C. Gentry, B. Lynn, And H. Shacham Are Presented A Effective Security System With Aggregate Signature Scheme On Bilinear Maps. The Bilinear Maps Contract Extra Structure And Power To Providing High Security. The Aggregate Signature Reduces Size And Communication Bandwidth. . The Aggregate Signature Describe With Aggregate Signature Scheme Based On Co-GDH Signature. Encrypted Signatures Evolved In Verifiably Encrypted Signature Scheme With Seven Algorithms. In The Seven Algorithms Three Of Them Are Ordinary Signature Scheme And Other Are Verifiably Encrypted Signatures

H . Privacy –Preserving Public Auditing for Secure Cloud Storage : Cong Wang, Sherman S, M. Chow, Qian WangKui Ren, and Wenjing Lou are proposes a privacy-preserving public auditing system for security data storage in Cloud. A homomorphic linear authenticator and the TPA would not have any knowledge about the cloud data storage. TPA handle multiple audit sessions from different users data. Privacy preserving system provides secure data storage. The data contents are stored in the TPA and the TPA audit the storage files and check the data uniqueness or matching contents. The main concept of this paper was batch auditing.

III. PROPOSED SYSTEM

In my paper cloud is most widely used for storage purpose and anyone can access the stored data from anytime, anywhere. Most probably shared data in the format of image or file types, cloud control and share the stored data to the user group. If an owner wants to sale his/her data in the cloud means the cloud and the data owner between and agreements. The private cloud services are services are pay and precede types. If the cloud contains many customers, then cloud provides the service after payment of a particular amount. In this case the cloud act as a marketing manager and the original user is silent and the cloud gives a particular benefit percentage to the data owner. One of the best ways to ensure confidential data is protected in the cloud is to utilize encryption for data. Almost all cloud service providers support encryption for information storage, but few offer support for data at ease. The encryption capabilities of the cloud service provider need to equal the degree of sensitivity of the data being hosted. Encryption plays a big role in fulfillment as many policies require specific data elements to be encrypted. The most important guidance on encryption is publicly available from NIST 800-111 and FIPS-140-2. These encryption standards can help you evaluate the encryption capabilities of a cloud provider for compliance with regulations to protect a user. Confidential data in the cloud, encryption is a powerful tool that can be used effectively. Only the user can confidently utilize cloud providers knowing that their confidential data is protected by encryption. But some private cloud contains encrypted files so the user cannot change or remove the unwanted part of the shared data. The main disadvantage is if the owner wants to upload the 10 file means the 10 files uploaded at the same time otherwise if the owner uploaded the two 5 files means the order will be changed. In this condition using homomorphic algorithm to edit the uploaded resource data for encrypted data change into a decrypted format.

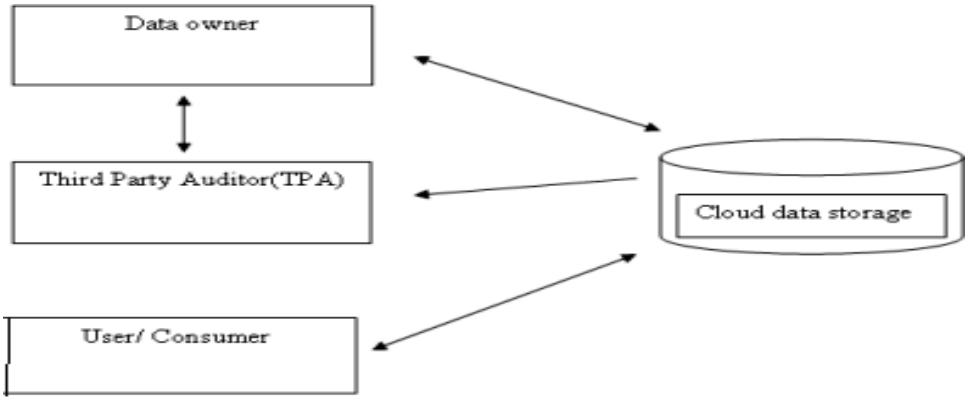

Fig. Preserving privacy and public auditing shared data in cloud environment

IV. DISCUSSION

Many of project works develop in previously which is only can store data, share data in multiple user and share data in a large number of users in a group. The purpose and develop a secure and efficient system with privacy protection of service. In this paper, propose a homomorphic algorithm and third party auditing scheme to construct a secure data management mechanism with high privacy protection method. In our scheme, the major merits are: (1) prevention abuses attacks; (2) data security; (3) privacy protection; (4) Auditing details to the data owner (5) word, index and content wise data searching is applicable.

V. CONCLUSION

In this paper, privacy-preserving public auditing mechanism for shared data in the cloud environment. The auditing is carried out by a trusted Third Part Auditor (TPA). The TPA might learn unauthorized information through the auditing process, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. Efficiently audit the integrity of shared data with dynamic groups while still preserving the identity of the signer on each block from the third party auditor. Also, using homomorphic algorithm to support word, index and content wise searching into the encrypted cloud data. In method provides data security and privacy of original data format .at the same time which help to the

REFERENCES

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

[2]. S. Yu, C. Wang, K. Ren, and W. Lou, *Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, inProc. IEEE International Conference on Computer Communications (INFOCOM)*, 2010, pp. 534–542.

[3]. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, *Scalable and Efficient Provable Data Possession, in Proc. International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2008.

[4]. C. Wang, Q. Wang, K. Ren, and W. Lou, *Ensuring Data Storage Security in Cloud Computing, in Proc. IEEE/ACM International Workshop on Quality of Service (IWQoS)*, 2009, pp. 1–9.

[5]. Boyang Wang, Baochun Li and Hui Li,*Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud*,2012.

[6]. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps, in Proc. In- ternational Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag*, 2003, pp. 416–432.

[7]. Wang, C., Chow, S., Wang, Q., Ren, K., & Lou, W,*Privacy-preserving public auditing for secure cloud storage*,2010.

[8]. D. Boneh and D. M. Freeman, *Homomorphic Signatures for Polynomial Functions, in Proc. International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT). Springer-Verlag*, 2011, pp. 149–168.

[9]. M. Armbrust, A. Fox, R. Griffith, A. D.Joseph, R. H.Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,*A View of Cloud Computing,Communications of the ACM,vol. 53, no. 4, pp*. 50–58, Apirl 2010.