ISSN:0975-9646

Preserving Public Auditing and Privacy Policy for Shared Data in the Cloud

Krishna Kumar L[#1], Deepa P Sivan[*2]

[#](Professor, Department of Computer science,
Nehru Institute of Technology/ Anna University, India)
*(Scholar, Department of Computer science,
Nehru Institute of Technology/ Anna University, India)

Abstract— Cloud computing technology providing services rather than a product that permits users to use applications without installation of applications and access their files, application on any personal computer, laptop, tab and mobile devices within the internet or intranet connection. Whereby the software, shared resources and information are provided as a utility network. The Cloud may share data in flexible manner across multiple users. **Cloud computing are an internet based sharing service. It has some benefits as avoidance of capital expenditure on personal maintenance, Hardware, software and relief of online burden data storage in a network. Many users can continuously access service from the remote locations. Cloud arises some issues in data security, privacy, integrity, dynamic updates. On the user side every time it is not possible to check their data consistency of stored data on cloud storage. The cloud server stores large amount of data which does not offer guarantees on data integrity and consistency. This problem is solved by a public auditing method, which ensure the integrity and to reduce online burden on cloud data storage. So that user can resort to Third-Party Auditor (TPA) to audit the data by using the ring signatures for data security. The preserving identity privacy of the signer on each block from the TPA means, the group is pre-defined before sharing data is created in the cloud. The membership of each user in the group is not changed during the data sharing stage. The original user is responsible for who is able to share his data before outsourcing data to the cloud. The TPA audits the integrity of shared data across dynamic groups of users in the cloud.**

Keywords— **cloud computing, privacy policy, preserving, public auditing, shared data, ring signature**

I. INTRODUCTION

Cloud computing technology contains a set of policy, which is related to its privacy, security, anonymity, reliability and liability etc. The most important privacy related to security and how cloud provides its service assurance. Currently, many frameworks and security models to ensure the security issues. In cloud computing there are different security issues, among them Data security is having its own importance, since the users are putting their sensitive data into third party storage. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The name of cloud computing comes from the cloud-shaped use as an abstraction for the complex type system infrastructure design. Clouds protect user's data with its remote services, software at any geographical areas. Cloud is long term vision in Information Technology and electronic-services. Cloud computing can expose its online services in flexible manner. Basically there are four different types of deployment models in cloud infrastructure. Cloud deployment models are public, private, community and hybrid. The public cloud is pure cloud and its provides off-premise by third party system. Public cloud deployment model is managed and controlled by third party or a service provider, user can access service from any area with the help of internet connection. Private clouds are managed by specific team of persons or a particular organization and which is provides pay-as-you-go manner e-services. The other two different kinds of deployment models are hybrid and community clouds. Community clouds are mainly traditional IT type infrastructure. Many enterprises are take the hybrid cloud approach by using public clouds for general computing, while customer or user data is kept within a private cloud, community cloud are more traditional IT infrastructure cloud. The strength of cloud computing is its data are centralized and outsourced type [2] .The main benefits of cloud computing is online data storage which relief from online burden data storage management, flexibility type service, data access from any geographical locations, reduce economic cost, on scalability demands, sharing resources, outsourcing mechanism, platform in-depended, avoidance of capital expenditure on personal maintenance, software and hardware.

Cloud is an online virtualized storage pool and any user can access data from there. Network linked devices such as mobile phone, tab and desktop computers can access and stored data from the cloud data storage. Users can simultaneously access various services from different geographical locations. So cloud arise some data issues related to its service model, integrity, dynamic updates, privacy and security. In user side it is not possible to check their data consistency of stored data on cloud storage every time. The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. The data contain privacy policy is partially overlap its security methods .The main issues related to this field is data privacy. Cloud contains some privacy preserving methods and public auditing schemes. Today many network users are developing different kind of data storage resources that can be used online for real time application usage and back up of missing data [5]. In cloud many user are access and stored their data in simultaneously. Cloud preserves privacy of each user's identity and their data from attackers or abusers.

Data protection is needed for the data in transit and in rest as well as a part of the good service. Cryptography is always chosen as the successful remedy for the data security. Encryption makes difficulty in sharing data. This can be overcome by introducing a proxy re encryption scheme in the cloud. A Proxy server is introduced to perform the re-encryption scheme augmented with certificate less public key cryptography, leverages cloud not only for data storage but also for secure key distribution for data sharing. It also ensures that the cloud cannot get the clear data encryption key during the transformation. Data owner generates proxy re encryption keys with all of its potential recipients and sends to a cloud resident proxy service, along with the encrypted data encryption key with its public key [9]. A re-encryption key is generated from the data owner's private key and a recipient's public key. Using the re-encryption keys, the cloud is then able to transform the encrypted data and encryption key to one that can be decrypted using an individual recipient private key. The re-encryption scheme reduces the response time by avoiding the extra encryption and decryption thereby improving the performance.

II. Related Work

Today, ninety percentages of the network data users are accessing cloud services from different remote locations to defending their information knowledge areas. Some issues are does not possible to check in the cloud. The private cloud storage at any time data users always needs to maintain data privacy and integrity. Service provided in the clouds are the separate data entities of the user and it's characteristic. The privacy preserving mechanism allows public auditing of shared data stored in the cloud [10]. Many of the projects develop previously can only store data, share data in multiple user or share data in a large number of users in a group or in a dynamic group of users like Knox. The privacy preserving mechanism can analysis and maintains the data consistency and integrity. Mainly three authors C.Wang, Sherman S, M. Chow, Q. W Ren, and W Lou are introduce many paper related to shared data security and privacy policy terms and how they are reach in this concept . Mainly they using a TPA using for auditing purpose and using homomorphic algorithms for more data security [1].

III. Cloud Data Acessing

Cloud is a wide network area, more than one user can store and access data at anywhere and anytime .so there is many chance to developing data privacy and security issues .Some of the privacy issues are Insufficient user control , Information disclosure, Unauthorized secondary storage, Uncontrolled data proliferation , Dynamic Provision etc. Insufficient user control is a data owner lacks control over their data in the cloud, especially when their data are accessed or processed in the cloud environment. The information disclosure is a disclosure of sensitive data while data moves across the cloud. Sensitive information may be user's identity, usage data, personal information, etc. Unauthorized secondary storage is the possibility of accessing and retrieving the sensitive information and backing up containing files. The uncontrolled data proliferation is defined as flows of data in the cloud are unpredictable and uncontrollable by the data owner. Dynamic Provision is a method defined as the legal responsible entity in the cloud to assure privacy which is remains unclear, due to the dynamic nature of the cloud. Also there is many security issues in the cloud data. Data proliferation is defined as the flow of data in the cloud is unpredictable and uncontrollable by the data owner [3]. Dynamic Provision is a method defined as the legal responsible entity in the cloud to assure privacy which is remains unclear, due to the dynamic nature of the cloud. The system security issues are access control, verification, the consumer can access device control, data access, monitor, data deletion verification as follows Access control verification is ensure only authorized user can access data from the cloud.

The consumer access device control is control of consumer access device or points as mobile phone, PAD, personal computer are secure enough. The data access monitor is ensuring whom, when and what data being accessed from Cloud by Cloud service provider. Data deletion verification is specifying data deleted must be the data owner rather than another user of Cloud. The group signature contains some properties are traceability, excludability, anonymity, correctness [4]. Traceability is a group manager determine valid signature and also determine which member of cloud signed in the particular cloud group. The group signature created by a group member cannot be attributed successfully to another and group manager cannot generate signature behalf of another group member. Anonymity is a group signature on message infeasible to determine which particular member of Cloud generated the signature. Correctness is a properly generated group signature which must be accepted by verification by the group manager.

IV. System Design

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. TPA having in charge of the system parameter generation as user revocation, user registration, data identity of Cloud system. 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 infrastructure act as a system and 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. 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 preferred user group. The data owner wants to sale his/her data in the cloud then the cloud and the data owner between an agreement. The private cloud provides pay and

use service method service. If the cloud contains many user and its service provide 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. This is the best ways to ensure data confidential is protected by the cloud is to utilize data encryption methods. But few offer support for data failure. The capabilities of the cloud service provider need to equal the degree of sensitivity of the data.

Data encryption has a big role in fulfilment as many policies require specific data elements. The guidance on encryption is publicly available from NIST 800-111 and FIPS-140-2. Encryption standards can help you evaluate the encryption capabilities of a cloud provider for compliance with regulations to protect a user. Encryption is a powerful tool that can be used data confidently [7]. But some private cloud contains encrypted files so the user cannot change or remove the unwanted part of the shared data. Main disadvantage is the data 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 changed. Here we can use homomorphic algorithm to edit the uploaded resource data for encrypted data change into a decrypted format.

V. SYSTEM ARCHITCTURE

The data processed on clouds are often outsourced, causing a number of issues related to privacy and security of cloud. Such fears are becoming a significant barrier to the wide adoption of cloud services. To solve this, it is essential to provide an effective mechanism for users to monitor the usage of their cloud data. If users need to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. The proposed work provides end-to-end accountability in highly distributed fashion. This combines the aspects of usage control, authentication and access control. Data owners can track whether the service level agreements agreed and enforce access and usage control rules.

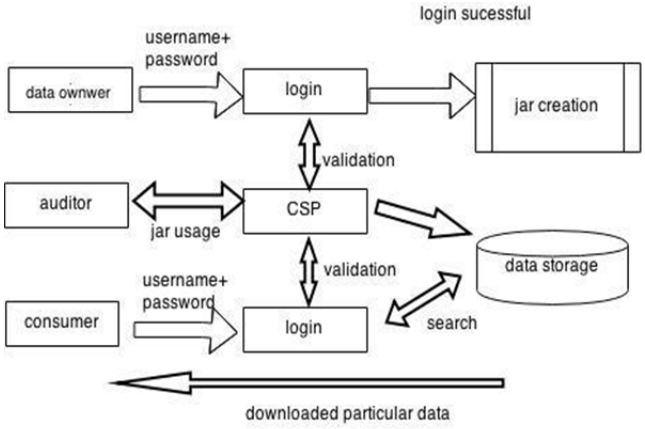

Figure1. Securing data proving method

We leverage and extend the programmable capability of JAR (Java ARchives) files to automatically log the usage of the users' data by any entity in the cloud. Users will send their data along with any policies such as access control policies and logging policies that want to enforce and enclosed in JAR files, to cloud service providers. Anyone access to the data will trigger an automatically authenticated logging mechanism local to the JARs.

Decentralized logging mechanism meets the dynamic nature of the cloud but also imposes challenges on ensuring the logging integrity. provide the JARs with a central point of contact which forms a link between the user. It recorded the error correction information sent by the JARs files, to monitor the loss of any log forms any of the JARs. The auditing is carried out by a trusted Third Party Auditor (TPA). The TPA might learn unauthorized information through the auditing method, mainly from data owners un-encrypted data in the cloud.

VI. RESULT AND DECISION

The auditing is carried out by a trusted Third Party Auditor (TPA). The TPA might learn unauthorized information through the auditing, especially from data owners unencrypted data auditing method in cloud . The auditing based on the authentication and authorization of the shared data in the cloud storage. Her we are using homomorphic algorithm, which is provide searching in word wise and index wise in encrypted format data. Many of the project works develop in previously which is only can store data, share data in multiple user or share data in a large number of users in a group or in a dynamic group of users. The privacy preserving mechanism which analysis and maintains the data consistency and integrity

VII. CONCULSION

In this paper, privacy-preserving public auditing mechanism for shared data in the cloud. The TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users. An interesting problem in our future work is how to 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 and using homomorphic algorithm to change the encrypted data into a decrypted format.

VIII. FUTURE WORK / FUTURE ENHANCEMENT

The interesting problems we will continue to study for our future work. One of them is traceability, which means the ability for the group manager (i.e., the original user) to reveal the identity of the signer based on verification metadata in some special situations.

REFERENCE

[1] B. Wang, B. Li, and H. Li, ―Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,‖ in Proceedings of IEEE Cloud 2012, 2012, pp. 295–302.

[2] 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, April 2010.

[3] K. Ren, C. Wang, and Q. Wang, ―Security challenges for the Public Cloud,‖ IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, ―Cloud Data Protection for the Masses,‖ IEEE Computer, vol. 45, no. 1, pp. 39–45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ―Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,‖ in Proceedings of IEEE INFOCOM 2010, 2010, pp. 525–533.
[6] B. Wang, M. Li, S. S. Chow, and H. Li, ―Computing Encrypted Cloud Data Efficiently under Multiple Keys,‖ in Proc. of CNSSPCC' 13, 2013, pp. pp.90–99.
[7] R. Rivest, A. Shamir, and L. Adleman, ―A Method for Obtaining Digital Signatures and Public Key Cryptosystems,‖ vol. 21, no. 2, pp. 120–126, 1978.
[8] The MD5 Message-Digest Algorithm (RFC1321). [Online] Available: https://tools.ietf.org/html/rfc1321
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ―Provable Data Possession at Untrusted Stores,‖ in Proceedings of ACM CCS'07, 2007, pp. 598–610.
[10] H. Shacham and B. Waters, ―Compact Proofs of Retrievability,in Proceedings of ASIACRYPT'08. Springer-Verlag,2008,pp.90–107.

.