Scientific Journal Impact Factor (SJIF) : 4.364
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745 ISSN (PRINT) : 2393 - 8161

PRIVACY-PRESERVING SYSTEM FOR SHARED DATA IN THE CLOUD ENVIRONMENT BY USING PUBLIC AUDITING SCHEME

Mr. Navaid Ahmed Khan[1] and Prof. V. B. Gadicha[2]

[1]*M.E. (Scholar), Department of Computer Science & Engg. P. R. Patil College of Engineering & Technology, Amravati*

[2]*Asst. Prof. Department of Computer Science & Engineering, P. R. Pote (Patil) Education and Welfare Trusts's College of Engineering & Management, Amravati*

Abstract-The Cloud computing is the internet based computing it enables sharing of services. It allows user to use application without installation of any application and user can access their personal files and application at any computer with internet or intranet access. However, public auditing for such shared data, while preserving identity privacy, remains to be an open challenge. Current system proposed the first privacy-preserving mechanism that allows public auditing on shared data stored in the cloud. In particular, proposed work exploit ring signatures to compute the verification information needed to audit the integrity of shared data. With current system 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 verify the integrity of shared data without retrieving the entire file and also provide the confidentiality to the shared data in cloud.

Keywords- Cloud Computing, Privacy-Preserving, Data Security, Data Integrity.

I. INTRODUCTION

Cloud Service Providers (CSP) provide the services to the users and also manage an enterprise infrastructure class that offers a scalable, reliable and secure environment to the users, and requires a very low marginal cost to the sharing nature of resources [1]. It is regular process for users to use cloud storage services to share data with others in team. Current system believes that sharing data among multiple users is perhaps one of the most engaging features that motivate cloud storage [2]. A unique problem introduced during the process of public auditing for shared data in the cloud is how to preserve identity privacy from the TPA, because the identities of signers on shared data may indicate that a particular user in the group or a special block in shared data is a higher valuable target than others [1]. Cloud resources are usually not only shared by multiple users but are also dynamically reallocated per demand. This can work for allocating resources to users, it is also necessary to ensure the integrity of shared data in the cloud is correct. [3]. During the process of accessing the data it is insufficient to detect and modify the data. Due to the storage, the server retains tremendous amount of data, in which little can be accessed. Data can be held long period of time during which there may be exposure to data loss. Than the client data the server has to store a large amount of data, but it is not necessary to have the same exact data [4]. As numbers of users are using such service provided by cloud service provider then the infrastructure ought to capable enough to support them and these resources ought to be shared between numbers of users. Data synchronization between number of users, service availability, and availability of data via any devices which includes browser facility make cloud more attractive [5]. The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server/ cloud service provider [6].

1.1. Motivation

Cloud computing is a computing model in which resources are provided to the users based on their demand. In cloud computing resources are provided by the cloud service provider known as CSP. Cloud has a number of users which daily uploading the data, user can also share the data with other users. So cloud needs a proper way of maintenance and security. TPA plays a role for maintain and analyzing the cloud properly, so it has motivated as proposed system can try to provide the privacy to all the documents and data and keep it secure from the unauthorized users, also maintain the data integrity in cloud. Proposed system is going to provide security to the data and user can share secured data with team members who are authenticated to access that data.

1.2. Objectives

Current dissertation is dedicated to achieve some of the following objectives.

- To achieve data privacy over the shared cloud environment to maintain confidentiality of user sensitive data.
- To identify & analyze the corrupted block of data in cloud via TPA.
- To implement secured data sharing by using ring signature.
- To build a secure mechanism for accessing shared data from the cloud.
- To implement public auditing scheme for shared data in the cloud, to maintain the integrity of data

II. LITERATURE SURVEY

2.1 Background History:

Cloud computing is becoming powerful network architecture to perform large- scale and complex computing. Cloud computing is the delivery of computing as a service rather than a product. The idea of providing a centralized computing service dates back to the 1960s, In 1966, Canadian engineer Douglass Parkhill published his book The Challenge of the Computer Utility, in which he describes the idea of computing as a public utility [7]. Consider Public auditability in their defined "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA based homomorphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file [5].

2.2 Existing System:

The first provable data possession (PDP) mechanism to perform public auditing is designed to check the correctness of data stored in an untrusted server, without retrieving the entire data. Moving a step forward, (referred to as WWRL) is designed to construct a public auditing mechanism for cloud data, so that during public auditing, the content of private data belonging to a personal user is not disclosed to the third party auditor [1]. Third Party Auditor (TPA) is available to verify user's private data for its integrity. TPA is also able to do audits for more than one user at same time and efficiently [8]. Recent visions of "cloud computing" and software as a service call for data, both personal and business, to be stored by third parties, but deployment has lagged [9]. Existing work introduced a dynamic audit service for integrity verification of untrusted and outsourced storages. Audit system can support dynamic data operations and timely anomaly detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table (IHT) [10]. Specifically, the data owner encrypts blocks of content with symmetric content keys. The content keys are all encrypted with a master public key, which can only be decrypted by the master private key kept by the data owner. The data owner uses his master private key and user's public key to generate proxy re-encryption keys [11].

III. PROPOSED WORK

3.1. Basic Idea:

In cloud data can be store in large scale and which can be shared as well it means that a single database can be controlled or access by single or multiple users at same instance. The data can be accessed by user as well at any time. The admin plays an important role in these things that is admin will decide the access of data to TPA. In such system for TPA it's necessary to maintain the security and integrity of data. So that system is going to perform the privacy preserving on to the all data which is shared with TPA for auditing, this will help to maintain data integrity for auditor and security over shared data. Thus to provide secure cloud storage supporting privacy-preserving many methodologies, frameworks and protocols have been proposed.

3.2. Proposed System:

The proposed system implementing various privacy preserving techniques over each and users data that is share with TPA and provide privacy preserving over cloud. In this TPA is able to maintain the auditing on the shared data and also check for data integrity without any information about user by using above techniques we can efficiently achieve followings. (1) Public Auditing: The third party auditor is able to verify the integrity of shared data without retrieving the entire data. (2) Correctness: The third party auditor is able to correctly detect whether there is any corrupted block in shared data. (3) Identity Privacy: During auditing, the TPA cannot distinguish the identity of the signer on each block in shared data.

TPA based approach to keep online storage honest. Proposed system uses the AES (Advance Encryption Standard) algorithm to preserve the privacy of user data. Like DES, AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption.

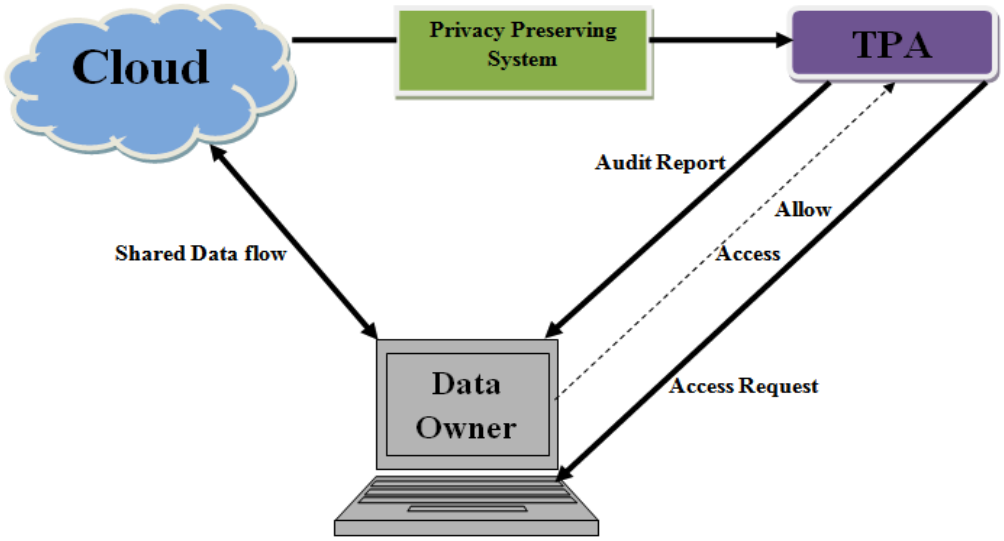

Fig. 1. System model

3.3. Result Analysis

In the proposed system we use the TPA (Third Party Auditor) which is used to perform the public auditing on the users data and maintain the integrity of that data and also preserve the privacy of user data and provide an efficient environment to the user to keep their data safe and easily accessible to them.

Table.1.Data extract from existing system

Is Encrypted	Encryption Algorithm Used	Output		
No	No	F_id	F_name	F_Director
		1	MINK	K Johar
		2	HNY	F Khan

As shown in table 1 in existing system TPA perform the query to retrieve the data from the database the data will be displayed as it is and it will seen by all no security is there for the user. In which TPA fire a query as "select * from film;" then he will get the record as present in the database

Table.2.Data extract from proposed system

Is Encrypted	Encryption Algorithm Used	Output		
Yes	Yes	F_id	F_name	F_Director
		?ü?ñ+a)e"fj?,	»ÀûÂ?Ù¾C:bi0bûÉ	Â9p?¿?FÜ»?
		?ü?ñ+a)e"fj?,	»ÀûÂ?Ù¾C:bi0bûÉ	Â9p?¿?FÜ»?

In proposed system TPA perform the query to retrieve the data from the database the data will be displayed in the encrypted format and security of user data will be achieved. In which TPA fire a query as "select * from film;" then he will get the record in the encrypted form from the database no one can read the data.

As shown in table 3 proposed system compares the various parameters with the existing systems and provides an efficient output for the user to keep their data safe from unauthorized access.

Table.3.Comparison of public auditing schemes in cloud

Comparison factor / Paper	C. Wang et al (2010)	Q. Wang et al (2012)	B. Wang et al (2013)	C. Liu et al (2014)	J. Yuan et al (2015)	H. Tian et al (2016	Proposed system
Authentication	NO	Yes	Yes	Yes	Yes	Yes	Yes
Availability	NO	NO	No	No	No	No	No
Protocol	NO	NO	No	No	No	No	HTTP
Technique	NO	BLS	Homomorphic authenticator based ring signature	Tags	Tags	Dynamic hash table	Tags
External Auditor	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encryption	NO	Yes	Yes	Yes	Yes	Yes	Yes
Data Structure Concept	Yes	Modified merkle hash tree	Merkle hash tree	Ranked merkle hash tree	No	Dynamic hash values	No
Signature	NO	Yes	Yes	Yes	Yes	Yes	Yes
Functions	Yes	No	No	No	Yes	No	Yes
Dynamism	Yes	Yes	Yes	Yes	No	Yes	Yes
Batch Auditing	Yes	Yes	Yes	Yes	Yes	Yes	No
Error Localization	NO	No	No	No	Yes	No	No
Data Recovery	NO	No	No	No	No	No	No

In existing system they are considering a single parameter for improvement of the system performance here we are performing operations on various parameters of the database with public

auditing scheme and the public auditing is perform by the TPA (Third Party Auditor) and it will display all the fields of database table in the encrypted form.

REFERENCES

[1] Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", Ieee 5th International Conference On Cloud Computing Year 2014.
[2] Mr. Kedar Jayesh Rasal, Dr. Shyamrao V. Gumaste, Prof.Sandip A. Kahate, "Effective Privacy-Preserving Public Auditing for Data Sharing in Cloud", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, July 2015.
[3] Dr. J. Suganthi, Ananthi J, S. Archana, "Privacy Preservation And Public Auditing For Cloud Data Using Ass", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November-December 2014.
[4] S.Karthikeyan, J.praveen And Mrs Sumathy, "Provable data possession for securing the data from untrusted server", Int. Journal of Engineering Research and Applications, Vol. 5, Issue 3, March 2015.
[5] Miss. Pratiksha Meshram Prof. Roshani Talmale Prof. G. Rajesh babu, "A System of Privacy Preserving Public Auditing for Secure Cloud Storage System", International Journal of Engineering Research & Technology (IJERT)
[6] Vol. 3 Issue 8, August – 2014.
[7] Sonali Bhausaheb Chemate, Mansi Bhonsle, "A Survey on Cloud Storage Privacy Preserving Public Auditing for Regenerating Code", International Journal of Science and Research (IJSR), Volume 4 Issue 12, December 2015.
[8] Monica R Kabra (Vivekanand Arts Sardar Dalipsingh Commerce and sciencecollege Aurangabad), "Basic concept of Cloud computing".
[9] Manoj Shantaram Tore, S.K.Sonkar, "A Cloud Storage System For Sharing Data Securely With Privacy Preservation And Fraud Detection", International Journal of Research in Engineering and Technology, Volume: 04 Issue: 08, August-2015.
[10] Hovav Shacham and Brent Waters, "Compact Proofs of Retrievability", in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008.
[11] Devi Parvathy Mohan, K.J.Jagdish, "Dynamic Audit Services for Outsourced Storages in Clouds", International Journal of scientific research and management (IJSRM), Volume 2, Issue 6, 2014.
[12] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing".

