Privacy-Preserving System for shared Data in the Cloud Environment by using Public Auditing Scheme: A Review

1. Mr. Navaid Ahmed Khan, 2. Prof. V.B. Gadicha

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

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

ABSTRACT

With cloud storage services, it is common place for data to be not only stored on the cloud, but also shared across multiple users. 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.

INTRODUCTION

Cloud computing is a type of internet based computing that provides shared computer processing resources and data to computers and other devices on demand, and provide the storage space to the users to store their documents, images, songs etc, can also retrieve whenever they want. But there is no surety about security of the document.

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. 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. 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 Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the datacenters that provide those services. The services themselves have long been referred to as Software as a Service (SaaS). The datacenter hardware and software is what we will call a Cloud. In general we heard about the public and private cloud. When a Cloud is made available in a pay-as-you-go manner to the general public, we call it a Public Cloud. We use the term Private Cloud to refer to internal datacenters of a business or other organization, not made available to the general public [2].

The authenticity of data can be emerged as a critical issue while storing data on the untrusted servers. The data can move from peer-to-peer storage systems, network file system, web-service object stores, and database systems. These kinds of systems prevents storage servers from mixed kind of representation and modifying data by analyzing and providing authenticity to check when accessing the data [3]. The archival storage requires many guarantees about the authenticity of data during the process of storage. 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 [4]. Infrastructures under the cloud are much more powerful and reliable than personal computing devices they are still facing the broad range of both internal and external threats for data integrity [5]. We formalize the related notion of ring signature schemes. These are simplified group signature schemes which have only users and no managers [6].

**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.

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

LITERATURE SURVEY
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
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]. Construct an aggregate signature scheme based on a recent short signature due to Boneh, Lynn, and Shacham (BLS) [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].

Limitations of Existing System

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Paper Title</th>
<th>Authors</th>
<th>Year Of Publishing</th>
<th>Methods Used</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Privacy- Preserving Public Auditing for Secure Cloud Storage [5]</td>
<td>Cong Wang, Sherman S.- M. Chow, Qian Wang, Kui Ren, and Wenjing Lou</td>
<td>2013</td>
<td>Public auditability</td>
<td>Do not consider the privacy protection of users’ data against external auditors. Indeed, they may potentially reveal user data information to the auditors.</td>
</tr>
<tr>
<td>2</td>
<td>Oruta; Privacy-Preserving Public Auditing for Shared Data in the Cloud [1]</td>
<td>Boyang Wang, Shaohua Li., and Hu Li</td>
<td>2014</td>
<td>Homomorphic authenticable signatures, not homomorphic signatures.</td>
<td>Signature schemes do not support blockless verification. Without blockless verification, the TPA has to download the whole data file to verify the correctness of shared data, which takes long verification times.</td>
</tr>
</tbody>
</table>
CONCLUSION

Cloud computing provide the storage space and the related services to the user by its own CSP (cloud service provider) and day by day it grows fast and every organization use cloud to store data and access whenever it required, so the cloud is best to manage our data at the remote system.

REFERENCES


[5]. Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE, “Privacy-Preserving Public Auditing for Secure Cloud Storage”.

[6]. Ronald L. Rivest, Adi Shamir, and Yael Tauman, “How to Leak a Secret”, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, MA 02139, rivest@mit.edu.

[7]. Monica R Kabra (Vivekanand Arts Sardar Dalipsingh Commerce and science college
Aurangabad), “Basic concept of Cloud computing”.
