© 2018 IJSRSET | Volume 4 | Issue 4 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Implementation On Privacy-Preserving Public Auditing for Shared Data in the Cloud

Urja Upadhyay, Disha Jaiswal, Neha Kumari, Bhagyashri Jawale
Computer Science & Engineering, Nagpur University, Nagpur, Maharashtra, India

ABSTRACT

In cloud computing, the way that organizations manage their data, due to its low cost and ubiquitous nature. Users access the application and enjoy the on-demand high quality information's and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. This paper introduces a cloud database storage architecture, this approach prevents the risk of both external and internal attack to the outsourced data. the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. Enhanced and secured third-party auditing, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. furthermore, TPA is trusted and capable of accessing the cloud storage to performed auditing. extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently, Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

Keywords : Data Storage, Privacy-Preserving, Public Auditability, Cloud Computing, Third Party Auditing(TPA).

I. INTRODUCTION

The User doesn't have to worry about storage. Maintenance of cloud data, But as data is stored at the remote place how users will get the confirmation about stored data. Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Cloud is used not only for storing data, but also the stored data can be shared by multiple users. Due to this the integrity of cloud data is subject to doubt. Cloud computing is very promising for the Information Technology application. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. 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 other. Ring signature is used to compute verification metadata needed to audit the correctness of shared data. With this, the identity of the signer in shared data is kept private from public verifiers.

II. EXSISTING SYSTEM

In this existing system, as data integrity and the security is main important thing in cloud, to provide full security and data integrity we are giving public auditing process. Our scheme performs both public auditing and data dynamic operation. The data dynamic performs operation like insert, update, and delete in block wise manner. TPA does the auditing process. Users without pre knowledge of the encrypted cloud data have go to through every retrieved file in order. So it reduces the time for auditing process. The traditional searchable encryption schemes to allow a user to securely search over encrypted data through keywords without first decrypting it. These techniques support only conventional Boolean keyword search. As there are problems like users load ,system crash , system failure at this situation multiple TPA do the auditing process in which if there is failure of one TPA another TPA. When directly applied in large collaborative data outsourcing cloud environment, they may suffer the following two main drawbacks. Which is absolutely undesirable in today's pay as you use cloud paradigm. In this scheme a group of users can access the CS and they share data in group. Any user in group does the update, delete operations. The system model for our scheme is given below.

A. The System Model:

The system model consist three different entities: the cloud user, the cloud server (CS) and the third party auditor (TPA).As shown in fig.1.A cloud user can be assigned more than one role. The cloud users manage the server accounts. Public auditing allows TPA along with user to check the integrity of the outsource data stored on a cloud. Privacy preserving allows TPA to do auditing without requesting for5 local copy of data. The TPA has capabilities and competence that the user does not have. They can also interact with cloud server to access the stored data for different purpose in different style. Every time it is not possible for user to check the data which is stored on cloud server that arrives online burden to the user .so that's why to reduce online burden and maintain that integrity cloud Figure 1.The architecture of cloud data Storage. User may resort to TPA. The data stored on cloud server is come from internal and external attacks, which is having data integrity threads like hardware failure, software bug, hackers, and management errors. The Cloud Server can maintain reputation for its self-serving. The CS might even decide to hide these data correction incidents to user.

B. Design Goals:

The data integrity and security can be achieved by enabling privacy public auditing for cloud data storage as given below:

1. **Privacy-preserving**: TPA can't see the user's data content during the auditing process.
2. **Public Auditability**: To allow TPA to verify the correctness of cloud data without demanding the copy of whole data.
3. **Batch Auditing**: TPA handles multiple users for multiple tasks during auditing process.
4. TPA performs auditing process with minimum communication.
5. **Identity privacy**: The TPA cannot identify the identity of the signer of each block when auditing process going on.

III. PROPOSED SYSTEM

In this project, we consider how to audit the integrity of shared data in the cloud with static groups. It means the group is predefined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing.

Problem Statement:

In our model, privacy is accomplished by allowing the parties to upload their data in multi clouds and data is split into multiple parts so it gives more protection.

Scope:

We are going to raise the privacy level of the data owner and the confidentiality of the data in a better way through the multiple cloud environments.

Advantages of Proposed System

1. We rouse people in general inspecting arrangement of information stockpiling security in Cloud Computing. Give a protection protecting reviewing convention.
2. To the best of our knowledge, our scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud.
3. We demonstrate the security and defend the execution of our proposed plans through cement tests and correlations with the state-of-the-symbolization.

IV. ARCHITECTURE

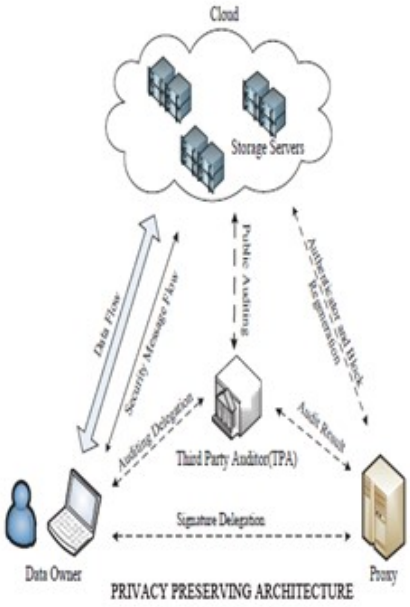

Figure 1

V. MODULES DESCRIPTION

1. vender

a) vender Registration:

In this module if a vender wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

b) vender Login:

If the vender is an authorized user, he/she can download the file by using file id which has been stored by data owner when it was uploading.

2. Owner

a) Owner Registration:

In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be able to do it. For that he needs to fill the details in the registration form. These details are maintained in a database.

b) Owner Login:

In this module, any of the above mentioned person have to login, they should login by giving their email ID and password.

3. Third Party Auditor

a) Third Party Auditor Registration:

In this module, if a third party auditor TPA (maintainer of clouds) wants to do some cloud offer, they should register first. Here we are doing like, this system allows only three cloud service providers.

b) Third Party Auditor Login:

After third party auditor gets logged in, He/ She can see how many data owners have upload their files into the cloud.

4. Data Sharing

We only consider how to audit the integrity of shared data in the cloud with static groups. It means the group is pre-defined before shared data is created in the cloud and the membership of users in the group is not changed during data sharing.

VI. MODULES

1.Owner registration

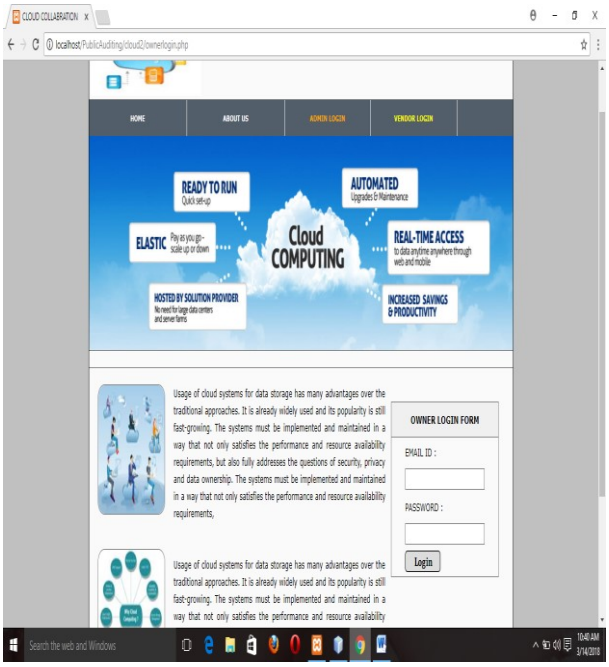

Figure 2

2.Vender registration

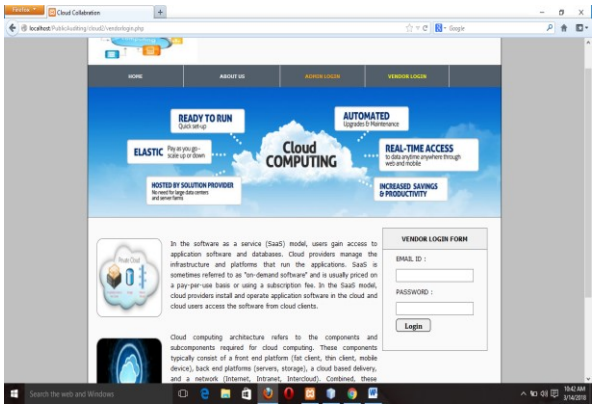

Figure 3

3.Public auditing in private cloud

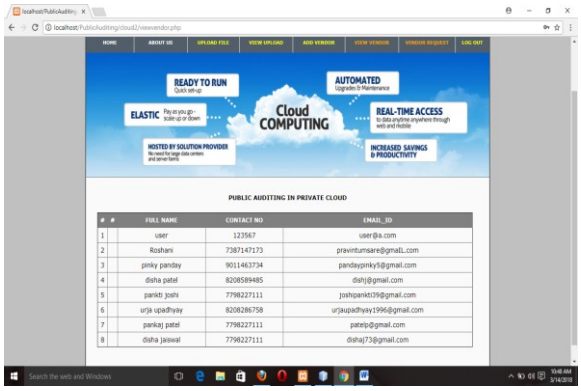

Figure 4

4.Collaboration file data

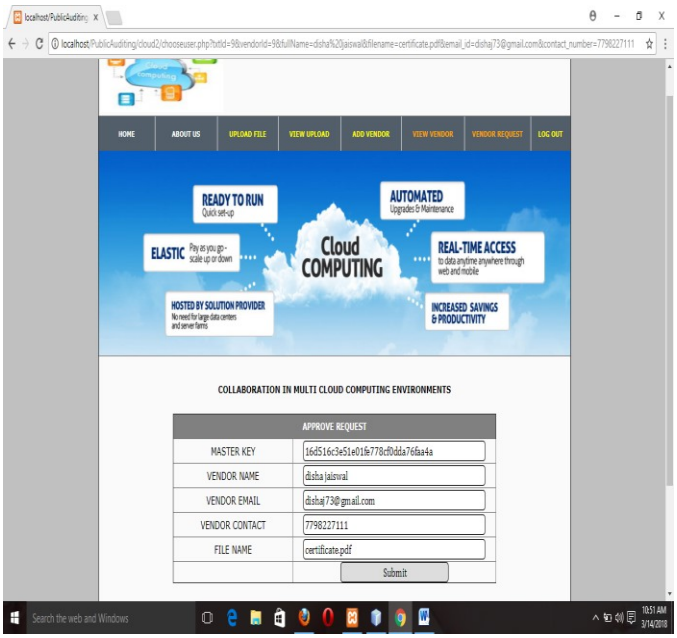

Figure 5

5.Request access module

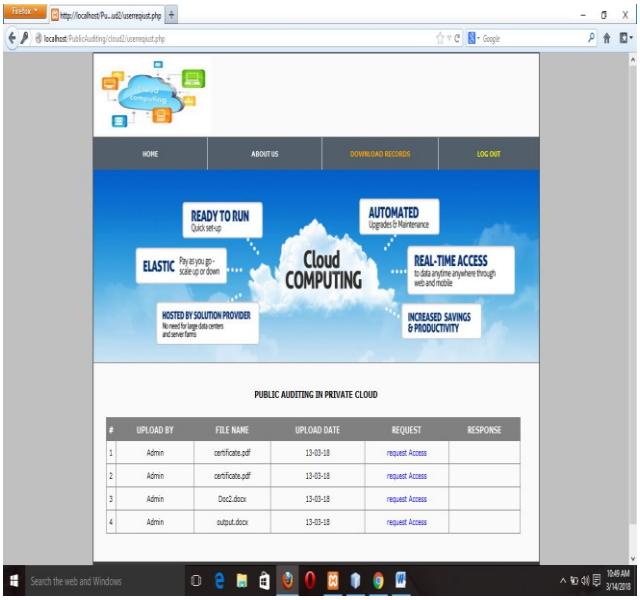

Figure 6

VII. CONCLUSION

The system is improved with result authentication and similarity based ranking model. The system also secures the search results. The system supports incremental. Searchable Symmetric Encryption scheme is used to provide storage and retrieval

security. Result authentication and similarity based ranking model. Extensive analysis shows that our schemes are provably secure and highly efficient. The data storage and search process is carried out with encrypted query model. Index operations on encrypted data values. The system also secures the search results .TPA may concurrently handle audit sessions from different users. Cloud customer can remotely store their data on a shared pool of configurable computing resources in cloud. The system supports incremental:

- ✓ Searchable Symmetric Encryption scheme is used to provide storage and retrieval security.
- ✓ Order preserving symmetric encryption schemes.
- ✓ Result authentication and similarity based ranking model.
- ✓ Index operations on encrypted data values.
- ✓ The system also secures the search results.

VIII. REFERENCES

[1]. S. Zerr, D. Olmedilla, W. Nejdl, and W. Siberski,Top-k Retrieval from a Confidential Index," Proc. Int'l Conf. Extending Database Technology: Advances in Database Technology (EDBT '09), 2009.

[2]. J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy Keyword Search over Encrypted Data in Cloud Computing," Proc. IEEE Infocom '10, 2010.

[3]. N. Cao, C. Wang, K. Ren, and W. Lou, "Privacy Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE Infocom '11, 2011.

[4]. C. Wang, K. Ren, S. Yu, K. Mahendra, and R. Urs, "Achieving Usable and Privacy-Assured Similarity Search over Outsourced Cloud Data," Proc. IEEE INFOCOM, 2012.

[5]. Cong Wang, Ning Cao, KuiRen and Wenjing Lou, "Enabling Secure and Efficient Rank Keyword Search over Outsourced Cloud Data" IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 8, August 2012.

[6]. Cong Wang, Qian Wang, KuiRen, and Wenjing Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," To appear, IEEE Transactions on Service Computing (TSC).

[7]. A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill. Order-preserving symmetric encryption. In Proceedings of Eurocrypt'09, volume 5479 of LNCS. Springer, 2009.

[8]. M. Li, S. Yu, N. Cao, and W. Lou. Authorized private keyword search over encrypted data in cloud computing. In Distributed Computing Systems (ICDCS), 2011 31st International Conference on, pages 383–392. IEEE, 2011.