IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Secure User Data Using Encryption for Preserving Private Data in Cloud

M Purnachandra Rao[1], P Srinivasa Rao[2], V Prasad[3]

[1, 3] (Department of Computer Science & Engineering, Raghu Institute of Technology, Visakhapatnam)
[2] (Department of Computer Science & Engineering, SV University, Meerut)

ABSTRACT

Cloud computing is internet based computing which enables sharing of services. Many users place their data in the cloud. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes. This data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. So, correctness of data and security is a prime concern. Here, the problem is considered for ensuring the integrity and security of data storage in cloud computing. Security in cloud is achieved by signing the data block before sending to the cloud. Using cloud storage, users can remotely store the data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public audit ability 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. In this paper, we proposed a secure cloud storage system supporting private preserving public auditing. The scheme is extended to support scalable and efficient public auditing in cloud computing. In particular, our scheme achieves auditing tasks from different users can be performed simultaneously by TPA. Here, the security is provided for proposed construction and justification to the performance of the scheme through concrete implementation and comparisons are produced.

Keywords: Cloud Computing , Storage , Authentication ,Third Party Author , Encryption & Blocks.

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 8, August 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

1. INTRODUCTION TO CLOUD COMPUTING:

Cloud computing is the use of computing resources that are delivered as a service over a network. The name came from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

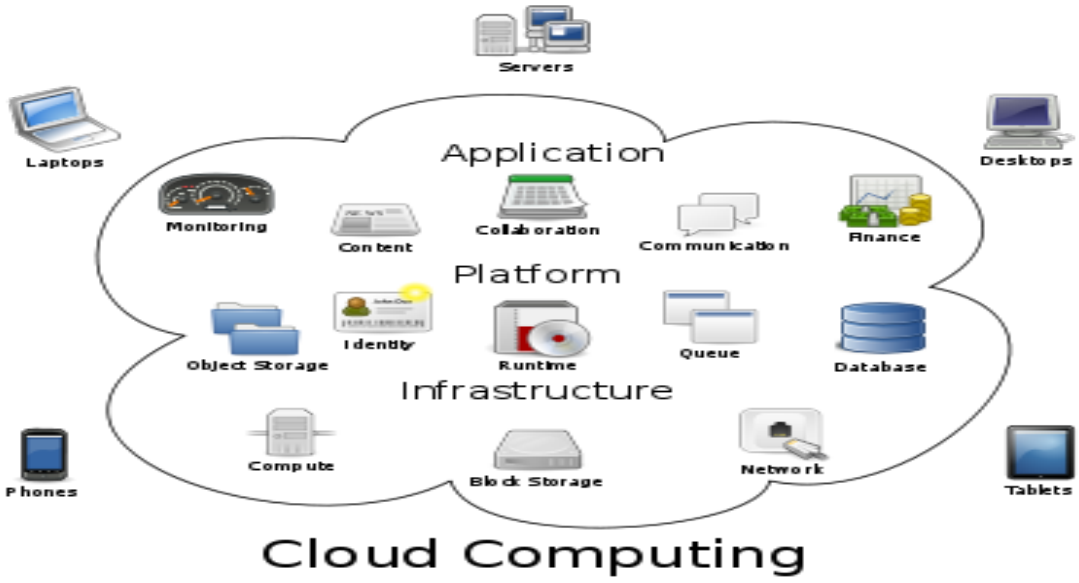

Figure 1.1 : Structure of Cloud Computing

The goal of cloud computing is to apply

- ✓ Traditional supercomputing.
- ✓ High performance computing power which is normally used by military and research facilities.
- ✓ To perform tens of trillions of computations per second in consumer-oriented applications such as financial portfolios.
- ✓ To deliver personalized information and to provide data storage for immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across

them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

1.1 PROPOSED SYSTEM :

In this proposed system we developed an efficient and dynamic data outsourcing on cloud by using the following three entities. They are :

• **Client:** An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, which can be either individual consumers or organizations.

• **Cloud Storage Server (CSS):** An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the client's data.

• **Third Party Auditor (TPA):** An entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

1.1.1 Advantages:

- ✓ We motivate the public auditing system of data storage security in cloud computing and propose a protocol supporting for fully dynamic data operations, especially to support block insertion, which is missing in most existing schemes.
- ✓ We extend our scheme to support scalable and efficient public auditing in cloud computing. In particular, our scheme achieves auditing tasks from different users can be performed simultaneously by the TPA.
- ✓ We prove the security of our proposed construction and justify the performance of our scheme through concrete implementation and comparisons.

2. DOMAIN ANALYSIS:

In this domain analysis section we deal with the aspects which strongly support the concept of cloud computing. They are :

A) Public audit ability for storage correctness assurance:

To allow anyone, clients who originally stored files on cloud servers, to have the capability to verify the correctness of stored data on demand.

B) Dynamic data operation support:

To allow the clients to perform block-level operations on the data files while maintaining the same level of data correctness assurance. The design should be as efficient as possible so as to ensure the seamless integration of public audit ability and dynamic data operation support.

C) Blockless verification:

No challenged file blocks should be retrieved by the verifier (*e.g.*, TPA) during verification process for efficiency concern.

D) Dynamic Data Operation with Integrity Assurance:

Now we show how our scheme can explicitly and efficiently handle fully dynamic data operations including data modification (M), data insertion (I) and data deletion (D) for cloud data storage. Note that in the following descriptions, we assume that the file "F" and signature have already been generated and properly stored at server. The root metadata "R" has been signed by the client and stored at the cloud server, so that anyone who has the client's public key can challenge the correctness of data storage.

E) Batch Auditing for Multi-client Data:

As cloud servers may concurrently handle multiple verification sessions from different clients, given K signatures on K distinct data files from K clients, it is more advantageous to aggregate all these signatures into a single short, one and verify it at one time. To achieve this goal, we extend our scheme to allow for provable data updates and verification in a multi-client system. The signature scheme allows the creation of signatures on arbitrary distinct messages. Moreover, it supports the aggregation of multiple signatures by distinct signers on distinct messages into a single short signature, and thus greatly reduces the communication cost while providing efficient verification for the authenticity of all messages.

F) Data Modification:

This is the most frequently used operations in cloud data storage. A basic data modification operation refers to the replacement of specified blocks with new data blocks. At start, based on the new block the client generates the corresponding signature. The client signs the new root metadata " R' " by sigsk(H(R′)) and sends it to the server for update. Finally, the client executes the default integrity verification protocol. If the Output is TRUE, delete sigsk(H(R′)),and generate duplicate file.

2.1 PROBLEM ANALYSIS :

To enable privacy-preserving public auditing for cloud data storage under the mentioned model, our protocol design should achieve the following security and performance guarantee:

1) **Public audit ability**: To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users.

2) **Storage correctness**: To ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing user's data intact.

3) **Privacy-preserving**: To ensure that there exists no way for TPA to derive user's data content from the information collected during the auditing process.

4) **Batch auditing**: To enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

5) **Lightweight**: To allow TPA to perform auditing with minimum communication and computation overhead.

.

2.2 FUNCTIONAL REQUIREMENTS:

The functional requirement of the system defines a function of software system and its components. A function is described as a set of inputs, behavior of a system and output.

2.2.1 INPUT DESIGN :

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy.

(1). **Input Design** is the process of converting user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and

show the correct direction to the management for getting correct information from the computerized system.

(2).It is achieved by creating **user-friendly** screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulations can be performed, which also provides record viewing facilities.

(3).When data is entered, it will check for its **validity**. Data can be entered with the help of screens. Appropriate messages are provided as when needed. Thus the objective of input design is to create an input layout that is easy to follow.

2.2.2 OUTPUT DESIGN:

A quality output is one, which meets requirements of end user and presents information clearly. In any system results of processing are communicated to users and to other system through outputs. In output design it is determined about the information displacement for immediate need and also about hard copy output. It is most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

(1). Designing computer output should proceed in an organized, the right output must be developed while ensuring that each output element is designed so that users will find the system functioning effectively. When analysis design computer output, they should identify the specific output that is needed to meet the requirements.

(2). Select methods for presenting information.

(3). Create document or report that contain information produced by system.

2.3 USER INTERFACE DIAGRAM:

User interface diagram (UID) is the design of user interfaces for machines and software such as computers, mobiles and other electronic devices, with the focus on maximizing the user experience. The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals.

The attributes of present information represent the static aspects of the interface and can be generally regarded as the look of the interface. The seven presentation attributes are:

- **Clarity:** The information content is conveyed quickly and accurately.
- **Discriminability:** The displayed information can be distinguished accurately.

- **Conciseness**: Users are not overloaded with extraneous information.
- **Consistency:** A unique design, conformity with user's expectation.
- **Delectability:** The user's attention is directed towards information required.
- **Legibility:** Information is easy to read.
- **Comprehensibility:** The meaning is clearly understandable, unambiguous, interpretable and recognizable.

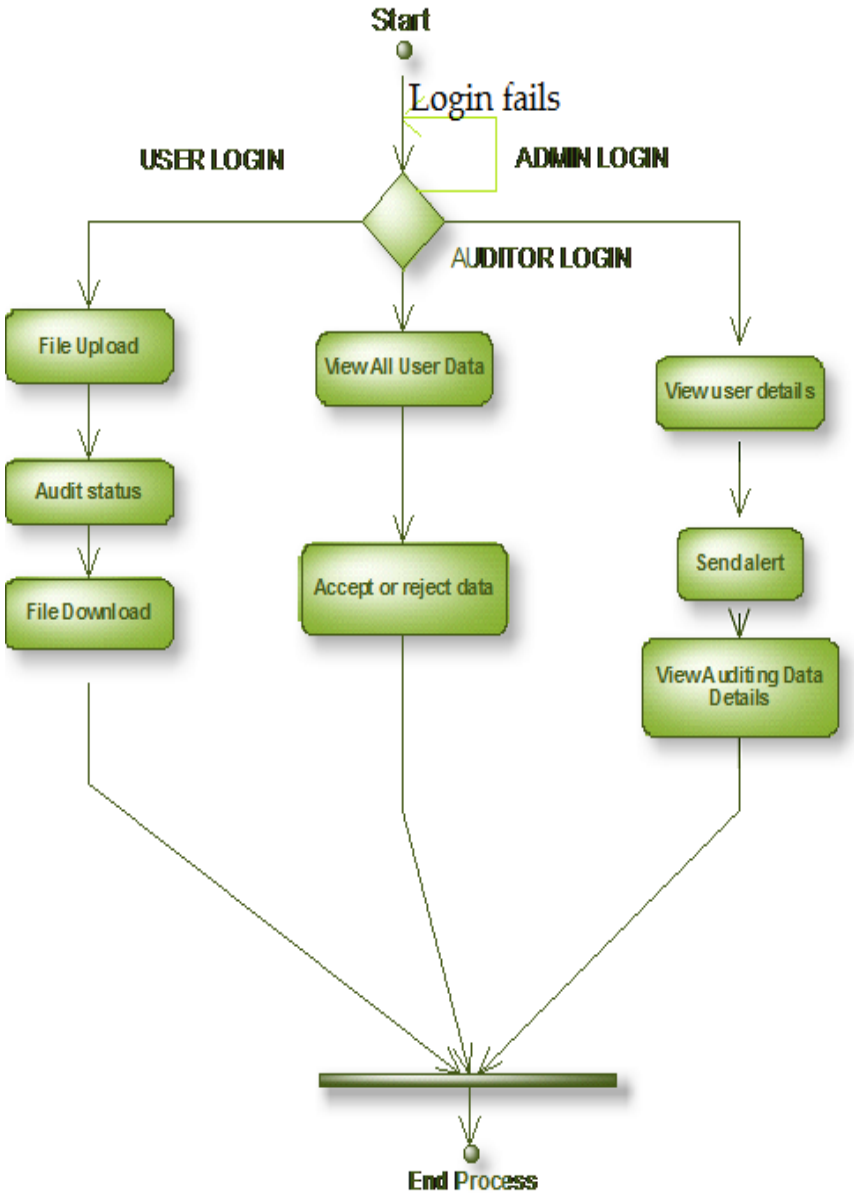

Fig 1.2: User Interface diagram

3. RESULTS :

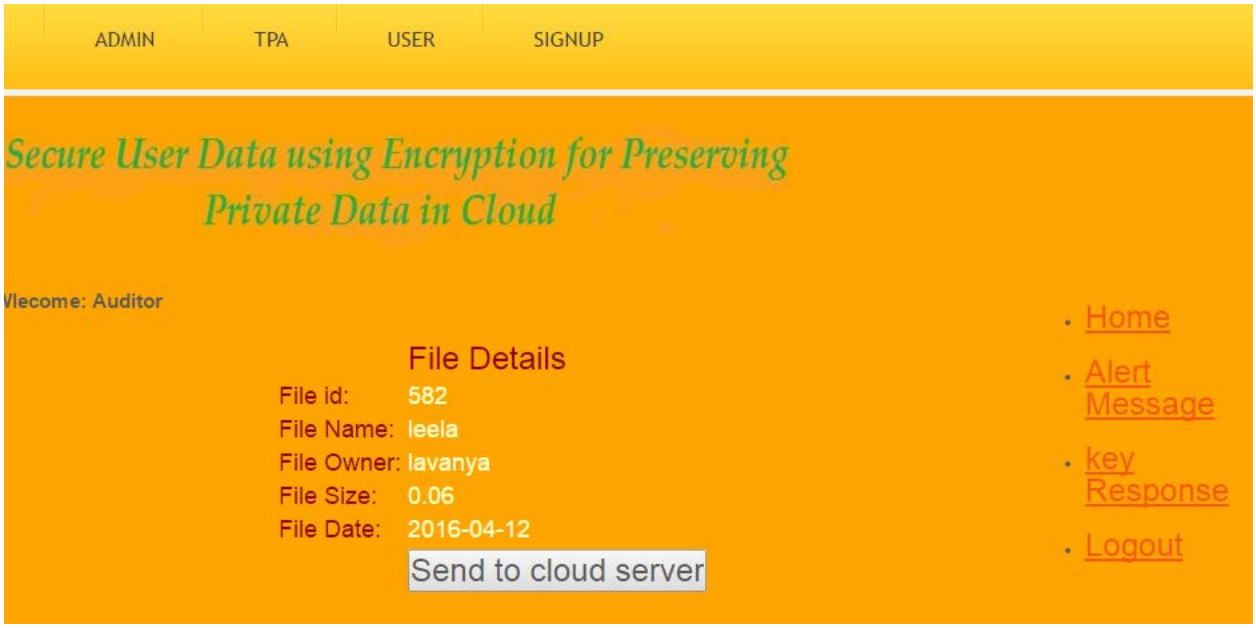

Fig 1.3: Once the auditor clicks on send to cloud server, then the alert message for admin will be received as :

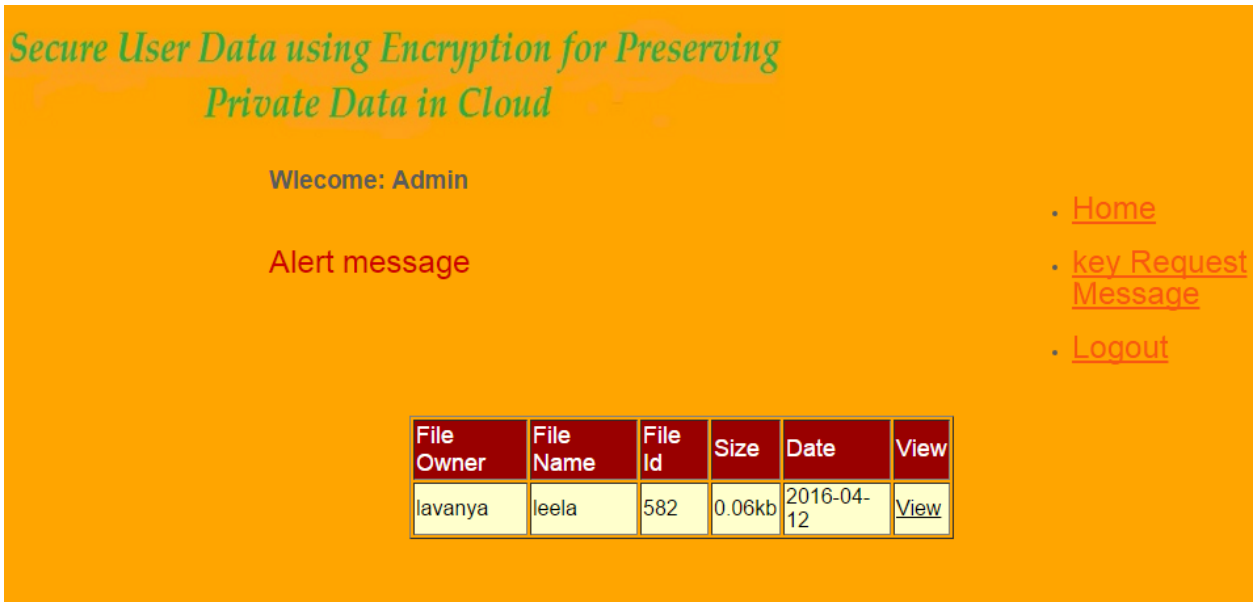

Fig 1.4: Then admin need to send the proof generation code to the TPA. That will be shown below :

Fig 1.5: Once the proof is generated then the next step is as below :

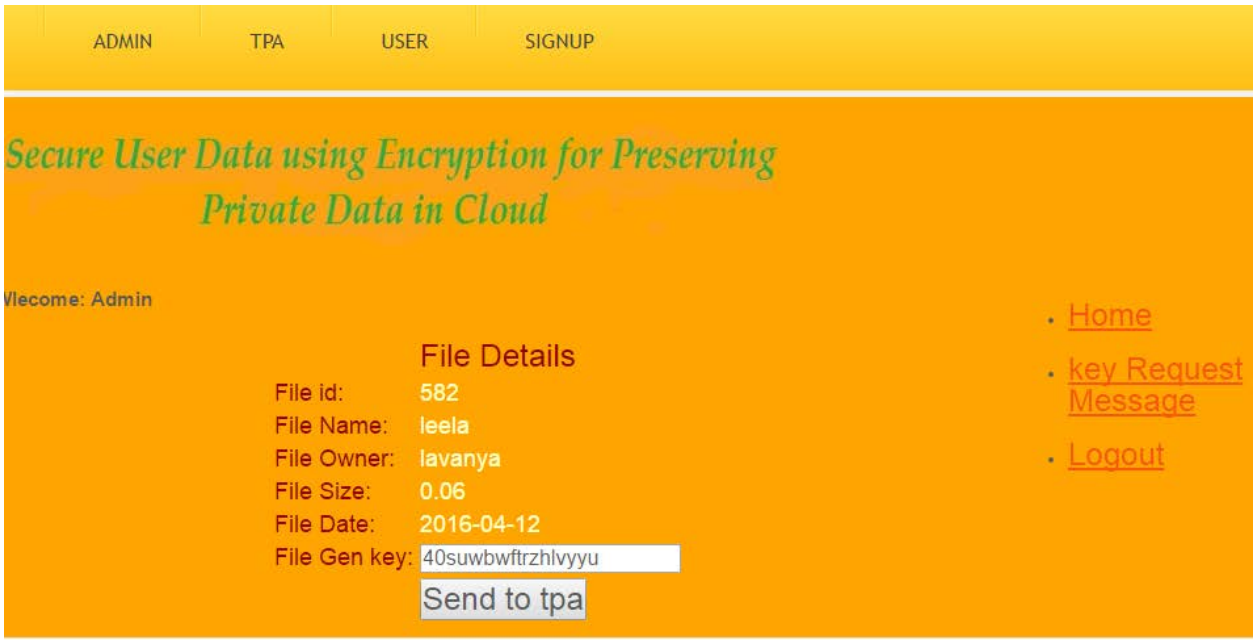

Fig 1.6: Then auditor receives that file as accepted by the admin or cloud as shown below :

Fig 1.7: After the acceptance of both the admin and TPA, the file will be stored in user database as shown below :

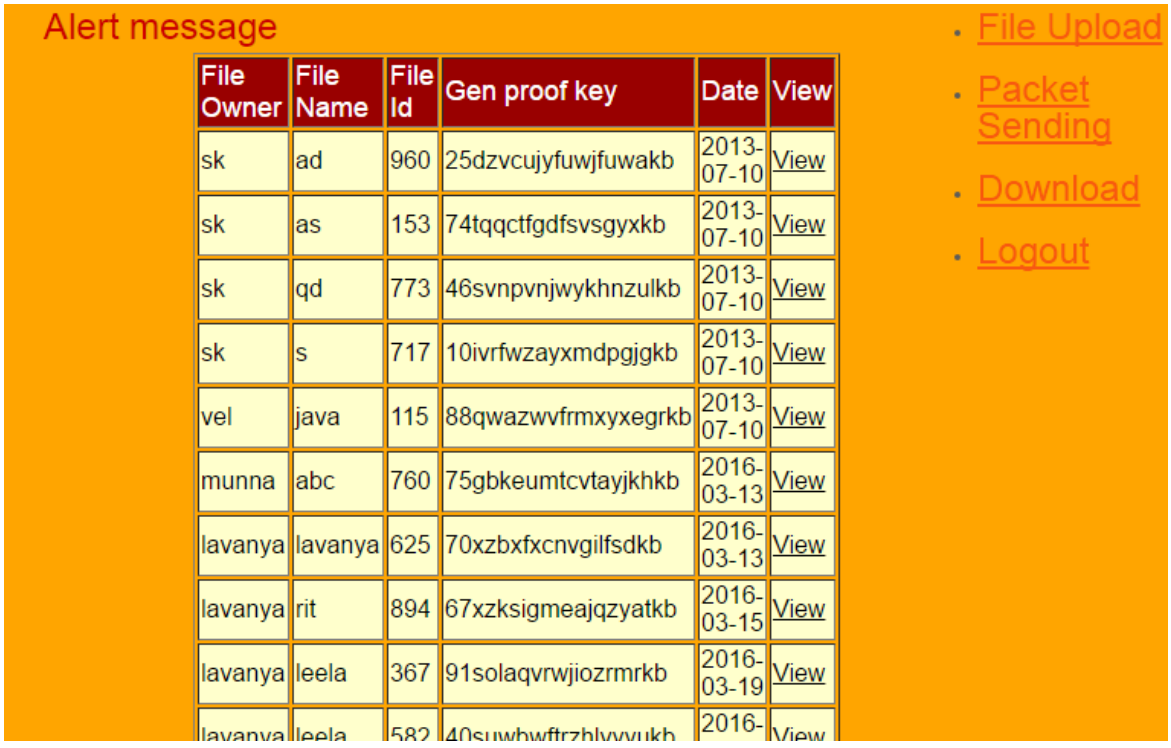

Fig 1.8: For the file to be downloaded by the user ,he need to login by his public audit ability key and need to download the file by giving the set of meta keys which were given before for retrieving the file from the database were shown in figure below.

CONCLUSION

We proposed a privacy preserving secure user auditing system for data storage security in cloud We utilize the homo-morphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users fear of their outsourced data leakage. TPA may concurrently handle multiple audit sessions from different users for their outsourced data files; we further extend our privacy preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

FUTURE ENHANCEMENT

Firstly, audit ability is defined as provable data possession (PDP) model for ensuring possession of data files on un trusted storages. This scheme utilizes the RSA based homo-morphic linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public audit ability in this scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, this protocol is not provably privacy preserving, and thus may leak user data information to the auditor. And also the number of audit challenges a user can perform is fixed before itself and public audit ability is not supported in this main scheme.

While all schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving secure user auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations. So, the future scope of the project is to enhance the batch auditing technique and also to allow a multi cloud storage so that the retrieval and processing of files can speed up and accessed much faster than before.

REFERENCES:

1. Madhubabu, Routhu, Vadamodula Prasad, and Andhra Pradesh. "IMPLEMENTATION OF DATA ACCESS CONTROL SCHEME FOR SECURE MULTI-AUTHORITY CLOUD STORAGE."
2. Prasad, V., Dr T. SrinivasaRao, and B. Sai Ram. "Information clustering based upon rough sets." *International Journal of Scientific Engineering and Technology Research (IJSETR)* 3 (2014): 8330-8333.
3. P. Mell and T. Grance, "Draft NIST working definition of cloud computing,"
4. Vahini, K., V. Prasad, and UV Chandra Sekhar. "Defend Data using ELGAMAL Digital Signature Data Decryption Algorithm." *IJCSIT) International Journal of Computer Science and Information Technologies* 5 (2014): 5062-5067.
5. 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, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
6. M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at Amazon.com, "Amazon s3 availability event: July 20, 2008.
7. Prasad, V., et al. "Comparative study of medical datasets IETD and UCITD using statistical methods." (2015).
8. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 598–609.
9. M. A. Shah, R. Swaminathan, and M. Baker, "Privacy preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
10. Infra, Human Motion Detection Using Passive. "Red Sensor." *International Journal of Research in Computer Applications & Information© IASTER* 2.2 (2014): 28-32.
11. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.
12. Prasad, Vadamodula, T. Srinivasa Rao, and PVGD Prasad Reddy. "Improvised prophecy using regularization method of machine learning algorithms on medical data." *Personalized Medicine Universe* (2015).
13. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
14. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009.
15. Prasad, V., et al. "Health diagnosis expert advisory system on trained data sets for hyperthyroid." *International Journal of Computer Applications* 102.3 (2014).

16. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, “Auditing to keep online storage services honest,” in Proc. of HotOS’07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.
17. Prasad, Vadamodula. "TamadaSrinivasaRao." Implementation of Regularization Method Ridge Regression on Specific Medical Datasets."."*International Journal of Research in Computer Applications & Information Technology* 3 (2015): 25-33.
18. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained access control in cloud computing,” in Proc. of IEEE INFOCOM’10, San Diego, CA, USA, March 2010.
19. Prasad, V., R. Siva Kumar, and M. Mamtha. "Plug in generator to produce variant outputs for unique data." *Int J Res Eng Sci* 2.4 (2014): 1-7.
20. A. L. Ferrara, M. Greeny, S. Hohenberger, and M. Pedersen, “Practical short signature batch verification,” in Proceedings of CT-RSA, volume 5473 of LNCS. Springer-Verlag, 2009, pp. 309– 324.
21. Prasad, Vadamodula, Thamada Srinivasa Rao, and Ankit Kumar Surana. "Standard cog exploration on medicinal data." *International Journal of Computer Applications* 119.10 (2015).
22. Prasad, V., T. Srinivasa Rao, and M. Surendra Prasad Babu. "Thyroid disease diagnosis via hybrid architecture composing rough data sets theory and machine learning algorithms." *Soft Computing* (2015): 1-11.
23. G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proc. of SecureComm’08, 2008, pp. 1–10.
24. C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in cloud computing,” in Proc. of IWQoS’09, July 2009, pp. 1–9.
25. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,” in Proc. of CCS’09, 2009, pp. 213–222.
26. R. C. Merkle, “Protocols for public key cryptosystems,” in Proc. of IEEE Symposium on Security and Privacy, Los Alamitos, CA, USA, 1980.
27. M. Bellare and G. Neven, “Multi-signatures in the plain public key model and a general forking lemma,” in ACM Conference on Computer and Communications Security, 2006, pp. 390–399.