Survey Paper related to Storage Security used in Cloud Computing

[1]Priyanka K. Deshmukh, [2]Prof. Imran R. Shaikh

[1]M. E. Student, [2]Asst. Professor, Dept. of Computer Engg. S.N.D. COE, Yeola. Maharashtra, India.

[1]*priyadeshmukh20.6@gmail.com*, [2]*imran.shaikh22@gmail.com*

Abstract - In cloud computing, data owners host their data on cloud servers, and users (data consumers) can access the data from the cloud servers. This new paradigm of data hosting service also introduces new security challenges that require an independent auditing service to check the integrity of the data in the cloud. Some existing methods for checking the integrity of the data cannot handle this problem efficiently and they cannot deal with the error condition. Thus, an secure and efficient dynamic auditing protocol should reject requests that are made with improper authentication. In addition, an excellent remote data authentication method should be able to collect information for statistical analysis, such as validation results. In this paper, first we design an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support dynamic data operations, which is efficient and has been proven to be secure in the random oracle model. We extended our auditing protocol further to support bidirectional authentication and statistical analysis. In addition, we use a better load distribution strategy, which greatly reduces the computational overhead of the client. Last, we provide an error response scheme, and our experiments show that our solution has good error-handling ability and offers lower overhead expenses for computation and communication than other approaches.

Keywords: Cloud computing, Storage security, Provable data possession, Bidirectional authentication.

I. INTRODUCTION

Cloud computing is a subversive technology that is changing the way IT hardware and software are designed and purchased [1]. As a new model of computing, cloud computing provides abundant benefits including easy access, decreased costs, quick deployment and flexible resource management, etc. Enterprises of all sizes can leverage the cloud to increase innovation and collaboration. Despite the abundant benefits of cloud computing, for privacy concerns, individuals and enterprise users are reluctant to outsource their sensitive data, including emails, personal health records and government confidential files, to the cloud. This is because once sensitive data are outsourced to a remote cloud, the corresponding data owners lose direct control of these data [2].

Cloud service providers (CSPs) would promise to ensure owners' data security using mechanisms like virtualization and firewalls. However, these mechanisms do not protect owners' data privacy from category of search function, including secure ranked multi-keyword search, fuzzy keyword search, and similarity search. However, all these schemes are limited to the single-owner model. As a matter of fact, most cloud servers in practice do not just serve one data owner; instead, they often support multiple data owners to share the benefits brought by cloud computing. For example, to assist the government in making satisfactory policies on health care service, or to help medical institutions conduct useful research, some volunteer patients would agree to share their health data on the cloud. Image Segmentation. In segmentation process the image contains labeling of pixel the image, then according to the assigned label classifying that pixel to the class to which it belongs. Segmentation in medical images can be done manually but it takes a lot of time as medical images are presented as stack called slices, which requires proper estimation of each and every slice of the image stack. By applying semi-atomic process a good result of segmentation can be obtained from a huge dataset of images. To preserve their privacy, they will encrypt their own health data with their secret keys. In this scenario, only the authorized organizations can perform a secure search over this encrypted data contributed by multiple data owners. Such a Personal Health Record sharing system, where multiple data

 DOI : 10.18231/2454-9150.2018.0013

owners are involved, can be found. The Data Owner(s) would worry that the data could be tampered (or deleted) in the cloud. They have this concern because they know that data can be lost in any infrastructure implemented. Later, in order to provide the function of the third-party validation, a third entity was added into the system model, i.e., the Third-Party Auditor. We propose an efficient remote data auditing method for securing the storage of big data in cloud computing. In addition to third-party verification, dynamic operation, and other functions, we also considered some other aspects, as discussed below.

II. LITRATURE SURVEY

A. Types of Cloud Systems and Actors

a) Actors

In[7] this Many activities use software services as their business basis. These Service Providers (SPs) make services accessible to the Service Users through Internet-based interfaces. Clouds aim to outsource the provision of the computing infrastructure required to host services. This infrastructure is offered ‗as a service' by Infrastructure Providers (IPs), moving computing resources from the SPs to the IPs, so to the SPs can gain in flexibility and reduce costs Depending on the type of provided capability, there are three scenarios where Clouds are used..

b) Infrastructure as a Service

In[3] this IPs manages a large set of computing resources, such as storing and processing capacity. Through virtualization, they are able to split, assign and dynamically resize these resources to build ad-hoc systems as demanded by customers, the SPs. They deploy the software stacks that run their services. This is the Infrastructure as a Service (IaaS) scenario.

c) Platform as a Service

Here[3] Cloud systems can offer an additional abstraction level instead of supplying a virtualized infrastructure, they can provide the software platform where systems run on. The sizing of the hardware resources demanded by the execution of the services is made in a transparent manner. This is denoted as Platform as a Service (PaaS). A well-known example is the Google Apps Engine [2].

d) Software as a Service:

Finally, there are services of potential interest to a wide variety of users hosted in Cloud systems. This is an alternative to locally run applications. An example of this is the online alternatives of typical office applications such as word processors. This scenario is called Software as a Service (SaaS).

e) GCa10 and GCb10

In this approach[3] superpixels are generated by stitching together overlapping image patches in such a way that each pixel should belong to only one of the overlapping regions. This method uses optimization approach which is very much similar to texture synthesis. GCa10 is used for generating compact superpixels which has control over the number superpixels and also it is useful for generating supervoxels. It has got three parameters which can become difficult to set them.GCb10 generates superpixels which are more compact than GCa10.Constant Intensity superpixels is used as a variant in this method.

B. Design Goals and Security Definitions

To enable privacy preserving ranked multi-keyword search in the multi-owner and multi-user cloud environment, our system design should simultaneously satisfy security and performance goals.

a) Ranked Multi-keyword Search over Multiowner

The proposed scheme should allow multi-keyword search over encrypted files which would be encrypted with different keys for different data owners. It also needs to allow the cloud server to rank the search results among different data owners and return the top-*k* results.

b) Data owner scalability

In scheme should allow new data owners to enter this system without affecting other data owners or data users, i.e., the scheme should support data owner scalability in a plug-and-play model

c) Data user revocation

Scheme should ensure that only authenticated data users can perform correct searches. Moreover, once a data user is revoked, he can no longer perform correct searches over the encrypted cloud data.

C) Efficient and Secure Dynamic Auditing Protocol for Integrity Verification In Cloud Storage

Computing, information homeowners host their information on cloud servers and users (data consumers) will access the information from cloud servers. As a result of the information outsourcing, however, this new paradigm of knowledge hosting service additionally introduces new security challenges, which requires associate freelance auditing service to ascertain the information integrity within the cloud. Some existing remote integrity checking strategies can solely serve for static archive information and, thus, can't be applied to the auditing service since the information within the cloud are often dynamically updated. Thus, economical and secure dynamic auditing protocol is desired to convert information homeowners that the information area unit properly holds on

 DOI : 10.18231/2454-9150.2018.0013

in the cloud. Economical and privacy-preserving auditing protocol was proposed to provide data integrity

a) Multi cloud storage

First we should create storage space for client to host there data in the cloud server. When storing the encrypted data in cloud server client fragment there data to reduce storage overhead. Fragmentation technique is the first process done by modified dynamic auditing protocol. During this fragmentation process we have to mention the fragmentation size of the data blocks. We further split the data blocks in to sectors. Sector size is restricted by the security parameter. Next step is to generate one data tag for each data block that consists of s sectors.

b)Modified Dynamic Auditing

Using key generation and tag generation algorithm we generate a computed data component.

KeyGen (λ) → (skh, skt , pkt). This key generation algorithm takes no input other than the implicit security parameter λ.

It outputs a secret hash key skh and a pair of secret-public tag key (skt , pkt). TagGen(M, skt , skh) → T.

The tag generation algorithm takes as inputs an encrypted file M, the secret tag key skt and the secret hash key skh. For each

c*) Data integrity and third party auditing:*

Chall (Minfo) → C. The challenge algorithm takes as input the abstract information of the data Minfo (e.g., file identity, total number of blocks, version number and timestamp etc.). It outputs a challenge C. Prove (M, T, C,Ti) → P. The prove algorithm takes as inputs the file M, the tags T and the challenge from the auditor C. It outputs a proof P. when sending proof we should include the time stamp to verify the validity of the data. Verify (C, P, skh, pkt ,Minfo) → 0/1. The verification algorithm takes as inputs the P from the server, the secret hash key skh, the public tag key pkt and the abstract information of the data Minfo. It outputs the auditing result as 0 or 1.

III. PROPOSED SYSTEM

We define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system to become a reality. Among various multi-keyword semantics, we choose the efficient principle of "coordinate matching. an excellent remote data authentication method should be able to collect information for statistical analysis, such as validation results.

Module:

Users:

There are two kinds of users in the System:

1. Data Owner-

Data owner Can Upload files in cloud file is encrypted at time of upload and secrete key generated with file.

2. Data User

Data Use can access files and Search files.

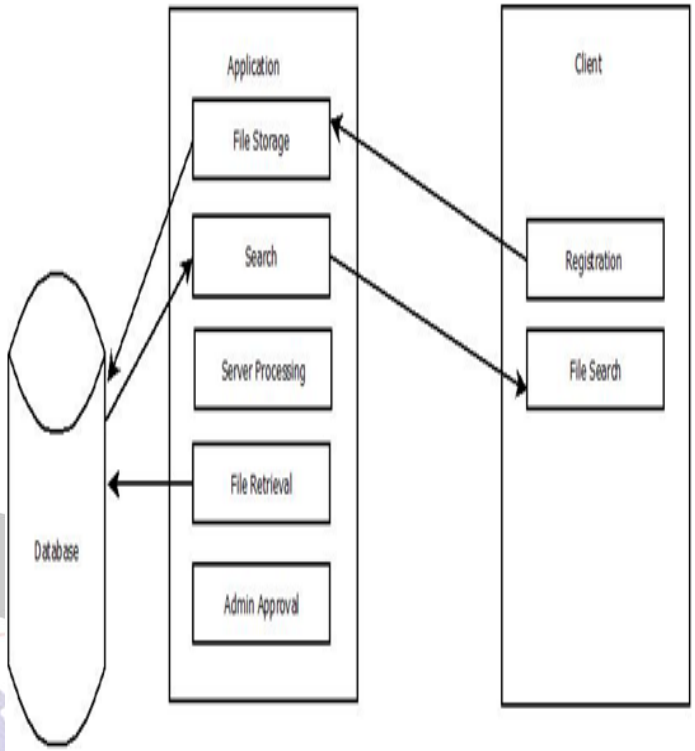

Fig 1 Block Diagram of System

Data Owner's Modules Description:

1) Login Module
2) Data Upload
3) View Files (Search)
4) File Share

IV. CONCLUSION

The previous work mainly focused on providing privacy to the data on cloud in which using multi-keyword ranked search was provided over encrypted cloud data using efficient similarity measure of co-ordinate matching. The previous work also proposed a basic idea of MRSE using secure inner product computation. There was a need to provide more real privacy which this paper presents. In this system, stringent privacy is provided by assigning the cloud user a unique ID. This user ID is kept hidden from the cloud service provider as well as the third party user in order to protect the user's data on cloud from the CSP and the third party user. Thus, by hiding the user's identity, the confidentiality of user's data is maintained.

 DOI : 10.18231/2454-9150.2018.0013

REFERENCES

[1] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM, pp. 829-837, Apr, 2011.

[2] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A Break in the Clouds: Towards a Cloud Definition," ACM SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50-55, 2009.

[3] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM, pp. 693-701, 2012.

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptograpy and Data Security, Jan.2010.

[5] A. Singhal, "Modern Information Retrieval: A Brief Overview," IEEE Data Eng. Bull., vol. 24, no. 4, pp. 35-43, Mar. 2001.

[6] I.H. Witten, A. Moffat, and T.C. Bell, Managing Gigabytes: Compressing and Indexing Documents and Images. Morgan Kaufmann Publishing, May 1999.

[7] D. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," Proc. IEEE Symp. Security and Privacy, 2000.

[8] E.-J. Goh, "Secure Indexes," Cryptology ePrint Archive, http:// eprint.iacr.org/2003/216. 2003.

[9] Y.-C. Chang and M. Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data," Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[10] R. Curtmola, J.A. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), 2006.

 DOI : 10.18231/2454-9150.2018.0013