PRIVACY PRESERVING OF ENCRYPTED CLOUD DATA USING BLOOM FILTER

VIJAYA KUMARI BOLLE [#1], VENKATA DURGARAO MATTA[*2]

M.Tech Scholar [#1], Assistant Professor [*2]
Department of Computer Science & Engineering,
Vishnu Institute Of Technology, Vishnupur, Bhimavaram,534202,

ABSTRACT

In current days cloud domain gained a tremendous increase of user‘s attention by several small and large scale companies including software, BPO, Schools, Colleges and a lot more. The cloud client try to adopt the centralized data storage and they will store their valuable data inside the cloud server with the help of interent. All the data is stored remotely and retrieved from the remote machines not from the local machines, hence the secrecy of data plays a vital role by the cloud service providers. As we all know that till now no cloud service provider is providing privacy for the data in terms of encryption and message digest in order to provide data authorization. Almost all companies try to search the data in a secure manner on remote cloud server. In general, the resultant query result may not be always correct due to dishonest cloud nature. As we all know that in current days cloud servers are almost dishonest in nature by omitting intentionally useful contents which are present in that file and they tell that due to some overhead space complexity we removed to save computational resources and communication overhead. In this paper, we also added a novel verification mechanism with the help of message digest algorithm in order to generate the message authentication code during file upload and download and in turn try to convert the data into decrypted manner. Here we also used a message digest algorithm SHA1 in which the short signature key is generated and used for verifying the data authentication. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical and efficient.

Key Words:

SHA1, Remote Location, Message Authentication, Message Digest Algorithm, Encryption, Data Integrity, Authorization, Cloud Server.

I. Introduction

Secure search techniques over encrypted cloud data allow a licensed user to question data files of interest by submitting encrypted query keywords to the cloud server during a privacy-preserving manner. In general the data results which came from the cloud query process agent may be sometimes correct and sometimes wrong and the returned query results may not be always positively generated within the dishonest cloud environment. For example, the cloud service provider who is dishonest in nature may intentionally remove the qualified [1]result of data to save the lot of space and then he try to add wrong content in the place of that genuine data. This may not be identified accurately by the cloud clients who are willing to view the file in plain text manner[2]. Hence a very strict and secure query system need to be provided, for identifying the data quality before it gets downloaded in the client PC. In this paper, we mainly design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the correctness of every file within the set but can also further check what percentage or which qualified data files aren't returned if the set is incomplete before decryption[3].

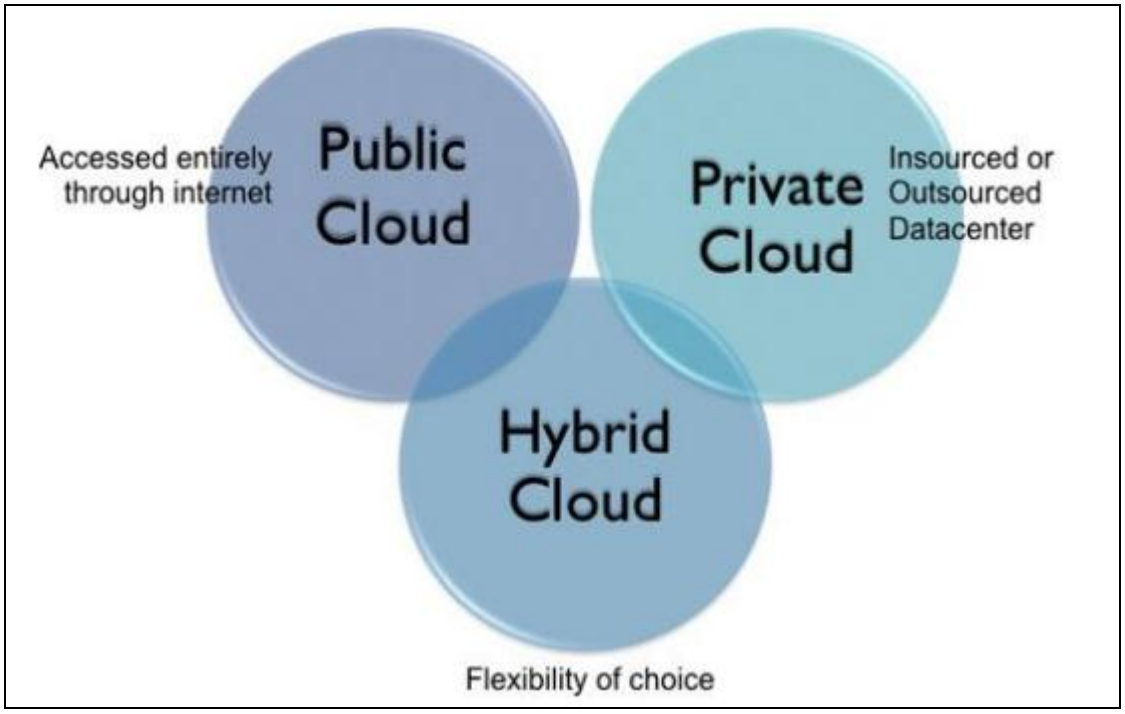

Figure 1.Repressent the Several Types of Cloud Providers Available for Data Storage

The verification scheme is loose-coupling to concrete secure search techniques and may be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data. Furthermore, a brief signature technique with extremely small storage cost is proposed to ensure the authenticity of verification object and a verification object request technique is presented to permit the query user to securely obtain the specified verification object[4]. Performance evaluation shows that the proposed schemes are practical and efficient. Now a day's almost all companies are moving their existing applications and their existing application databases into the cloud and start to enjoy many novel advantages that were provided by the cloud computing domain[5], such as on-demand computing resource configuration, easy and flexible access, saving a lot of software installation space , etc.

From the above figure 1, we can clearly identify that cloud service providers are providing us with three different types of storage areas, where each and every service differs with some small differences. Initially if we come across the public cloud this is always accessed entirely through the internet and we can open source access the data from remote locations without any restrictions[6] for accessing the files from this public cloud. Now if we come with private cloud this will be having the facility to access the file either from onward or inward and then store the file in remote location for accessing the file.And the third type of service which is provided by the cloud server is hybrid cloud which is clearly have the choice of storing the data under the clients decision.Hence all these three different cloud service providers try to provide an alternate solution for the end users in accessing the files from remote locations as per the clients need[7].

II. BACKGROUD WORK

In this section we mainly discuss about the related work that was carried out in give data authority and maintain integrity for the data in the cloud server. Now let us discuss about this in detail as follows

PRELIMINARY KNOWLEDGE

There are mainly 4 different services available in the cloud and one among them is DaaS which is the main service that what we are using now for providing security for the current application that and prove that this service also gives the best security for the data which is

stored inside the cloud memory locations [10], [11]. Now let us discuss about each and every service in detail as follows:

A. IaaS (Infrastructure as a Service)
B. PaaS(Platform as a Service)
C. SaaS(Software as a Service)
D. DaaS (Data /Data Base as a Service)

A. IAAS (INFRASTRUCTURE AS A SERVICE)

This is the first service out of various services that are available in the cloud. This service mainly deals with application level and it is basically used to set the infra-structure for the users. This service is mainly used to create infrastructure for the set of PCs that are linked in an area. The persons who come under this service is IT Professionals, this is clearly shown in the figure 3.

B. PAAS (PLATFORM AS A SERVICE)

The second important service in the cloud computing is Platform as a Service, where this is mainly used for customization of cloud server. Here in this service we try to set the platform for the users, where the developer comes under this service. Here the cloud server customizes which type of platforms is needed for their company usage is seen in this service.

C. SAAS (SOFTWARE AS A SERVICE)

The third service one among the best services in cloud computing is Software as a Service, where this is mainly used for a consumer to use the cloud service provider's applications running on a cloud IaaS. Generally business end-users come under this service where all the software's that are required for running the cloud are processed in this service.

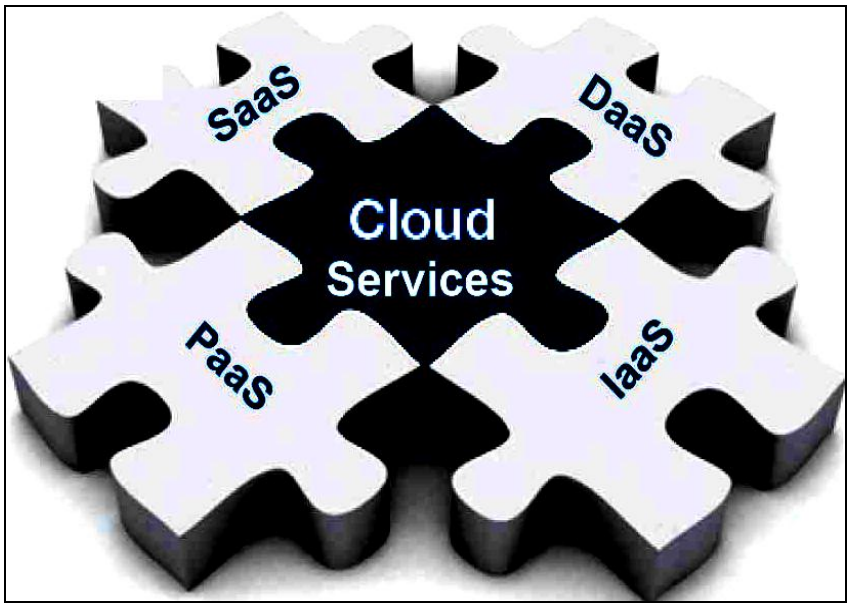

Figure.2. Represents the Different Cloud Services

D. DAAS (DATA/DATABASE AS A SERVICE)

This is the last one among the set of cloud services that was launched and included in various cloud client services is DaaS, which is clearly seen in above figure 2.This DaaS service is used mainly for storing the data in the form of encrypted manner [8]. As this is having various advantages compared with other cloud client services, it has a small limitation like the data which is stored in this DaaS is not stored in the encrypted manner which is stored in the plain manner. So in this proposed thesis we try to encrypt the data before it is uploaded into the cloud using DaaS service[9].

III. PRIVACY PRESERVING OF ENCRYPTED CLOUD DATA USING BLOOM FILTER

In this section we will mainly discuss about proposed model for which can guarantee the privacy preserving of encrypted cloud data by using the bloom filter. Here we can able to get the data under a secure manner from remote locations despite of accessing the modified file or altered file which is generated from the client.

System Model

The proposed model has three main entities like

1. Data Owner /Data Provider
2. Search User /Data Consumer
3. Cloud Server / Storage Provider

Initially the data owner is the person who may be an individual or sometimes an enterprise, who wishes to outsource a collection of documents

D = (D1, D2, . . . , Dn)

As we try to encrypt the documents before we upload into the remote server[10],hence the documents are termed as

C = (C1, C2, . . . , Cn) to the cloud server which are almost encrypted manner

The documents are labeled with some terms like D1,D2 and so on in order to identify the privacy of the documents.

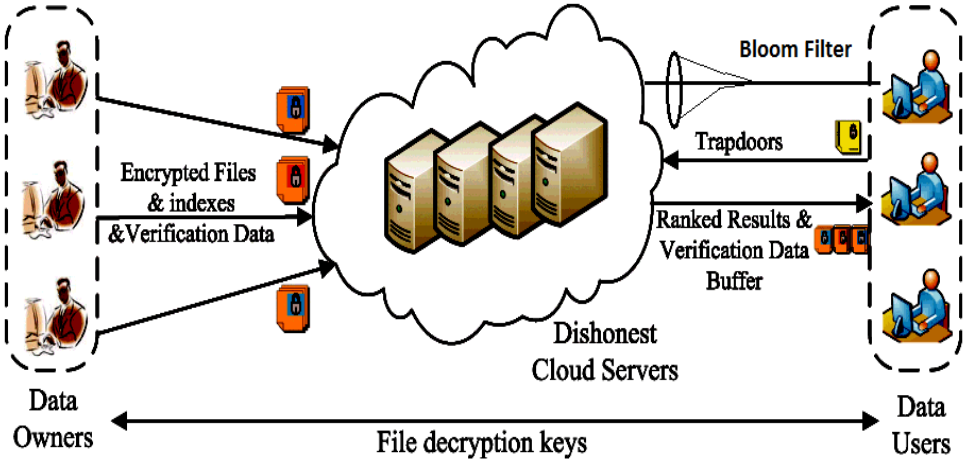

Figure.3. Represents the Proposed Architecture

From the above 3,we can clearly find out that there are multiple data owners and multiple data users available in the cloud architecture ,where the data owner try to insert all the data into the cloud server in an encrypted manner .

The data owner try to apply verification technique on the encrypted data in order to generate the short signature and identify the integrity for the data.

Here we can clearly see a main advantage in the current architecture, there is a bloom filter which tries to filter the files which are coming from the cloud server to the data user. This bloom filter acts as a filter agent in finding any altered or modified content which is present in the cloud server.

If the data user get an altered or modified data from the cloud server, then the bloom filter will identify such documents and immediately he will ignore that document and he will try to recover the original file which is uploaded by the data owner and then he will try to send the data user the original file which is not altered or modified by the dishonest cloud server.

In this way we can able to provide the privacy of data to the clients documents which are shared and accessed from remote systems under a centralized manner.By using this proposed architecture we can able to achieve high level of data security and data integrity is clearly maintained by the end users.

4. CONCLUSION

In this proposed thesis we finally implemented and analysed a novel verification mechanism with the help of message digest algorithm in order to generate the message authentication code during file upload and download and in turn try to convert the data into decrypted manner. Here we also used a message digest algorithm SHA1 in which the short signature key is generated and used for verifying the data authentication. By conducting various experiments on our proposed model, our result clearly tells that our proposed system is practical in providing data security and this is greatly helpful to achieve the data integrity by the remote clients who try to access the file from remote locations.

5. REFERENCES

[1] Two well known authors,K. Ren, and W. Lou, have written a paper on "Achieving secure, scalable, and fine-grained data access control in cloud computing," and they published in Proc.IEEE Conf. Comput. Commun., 2010, pp. 1–9.

[2] Two well known authors, S. Kamara and K. Lauter, have written a paper on "Cryptographic cloud storage," and they published in Proc.14th Int. Conf. Financial Cryptography Data Security, 2010, pp. 136–149.

[3] Two well known authors Wagner, and A. Perrig, have written a paper on "Practical techniques for searches on encrypted data," and they published in Proc. IEEE Symp. Security Privacy,2000, pp. 44–55.

[4] Two well known authors ,Y.-C. Chang and M. Mitzenmacher, have written a paper on "Privacy Preserving Keyword Searches on Remote Encrypted Data," and they published in Proc. Third Int'l Conf. Applied Cryptography and Network Security, 2005.

[5] Two well known authors ,Y. Huang and L. Malka, have written a paper on "Faster secure two party computation using garbled circuits," and they published in Proc. 20th USENIX Conf. Security Symp., 2011, p. 35.

[6] A well known author C. Gentry, have written a paper on "A fully homomorphic encryption scheme," and published in Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA,USA, 2009.

[7] A well known author, Raul Isea have written a paper on "The Present-Day Meaning Of The Word Bioinformatics", and published in Global Journal of Advanced Research, 2015. 554-568, Apr. 2006.

[8] Two well known authors ,P. Mell and T. Grance, have written a paper on "The nist definition of cloud computing," and published in http://dx.doi.org/10.602/NIST.SP.800-145.

[9] Two well known authors, K. Ren and Q. Wang, have written a paper on "Security challenges for the public cloud," and published in IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[10] Two well known authors, S. Kamara and K. Lauter, have written a paper on "Cryptographic cloud storage," and published in Springer RLCPS, January 2010.

6. ABOUT THE AUTHORS

VIJAYA KUMARI BOLLE is currently pursuing her 2 years M.Tech in Department of Computer Science & Engineering at Vishnu Institute of Technology, Vishnupur, Bhimavaram, 534202.Her area of interest includes Computer Networks, Java, Cloud Computing, Network Security

VENKATA DURGARAO MATTA is currently working as an Assistant Professor in Department of Computer Science & Engineering at Vishnu Institute of Technology, Vishnupur, Bhimavaram, 534202. He has more than 8 years of experience in teaching field. His resarch interest includes Internet of things, cloud computing, computer networks and network security.