A Novel Approach for Providing Data Security and Integrity over Encrypted Cloud Data

TANAGALA AJAY DEERAJ[#1] & V.SARALA[#2] & D.D.D.SURIBABU[#3]

[#1] MCA Student, Master of Computer Applications, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Science, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#3] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.

Received: January 13, 2019 Accepted: February 20, 2019

ABSTRACT: *Now a day's cloud domain gained a tremendous increase of user's attention by several small and large scale companies including software, BPO, healthcare, schools, colleges and a lot more. 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. In current days cloud servers are almost dishonest in nature by omitting intentionally some qualified results to save computational resources and communication overhead. In this paper, we proposed and analyzed 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 quality of each data file but also authorization of data by using MD5/SHA1 Algorithm (message digest algorithm) in which the short signature key is generated and used for verifying the data authentication.*

Key Words*: Message Digest Algorithm, Encryption, Data Integrity, Authorization, Cloud Server.*

I. Introduction

Now a day's cloud computing have occupied a major role in each and every part of the information processing and information storage centers. Although the cloud has became a valuable resource for all parts of information processing centres, there are some limitations with the cloud servers as all the data which is uploaded by cloud users will be automatically stored on the remote systems not on their local hardware, and can be accessed remotely via internet by connecting various intermediate servers. As the data is stored from our local hardware to remote hardware located at client location, the data user need to retrieve the data from the remote server, whenever he/she want any data from that remote hardware[1]. If we look at any of the various cloud service providers that are available in real time environment, all the CSP try to store the sensitive data in plain text manner in their storage area, either for public cloud users or private cloud users. So this will lead to no security for accessing the data in the current cloud servers for storing their valuable and sensitive information into its memory locations.

Figure.1. Represents Some of the Real-Time Cloud Service Providers Available in the Real Time Environment

In recent days 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, such as on-demand computing resource configuration, easy and flexible access, saving a lot of software installation space , etc. For each and every upload, the cloud users are more concentrated with one feature like privacy of their data. So in this paper we mainly concentrate on a new principle like encryption-before-outsourcing ,which has become a major fundamental attribute for giving privacy for the data which is uploaded by the various cloud owners into the cloud server (CS) [2], [3], [4], [5]. However, how the encrypted data can be effectively utilized then becomes another new challenge. Significant attention has been given and much effort has been made to address this issue, from secure search over encrypted data [6], secure function evaluation [7], to fully homomorphic encryption systems [8] that provide generic solution to the problem in theory but are still too far from being practical due to the extremely high complexity.

From the above figure 1, we can clearly find out various types of real time cloud service providers that are available for storing the valuable data in the real time environment. In our proposed thesis we use DRIVEHQ as the storage service for storing and accessing the files from application .As we use DRIVEHQ as storage medium ,it is also known as hybrid cloud because it will provide both public access and private access for the registered users.Initailly if any user registered into this drivehq server, he/she will get 1 GB of space for storage as a public access and once the data user crosses his usage more than 1 GB ,then immediately the current account will charge the corresponding user based on his excess storage.The storage cost depends on the current usage of the end user. Hence this DRIVEHQ provides a public account till 1 GB and it becomes a private account after 1 GB.

II. Related 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.

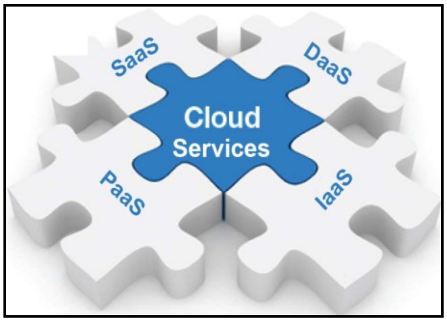

Figure.2. Represents the Various Cloud Services that are available in Real Time Cloud

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 [12]. 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.

III. Proposed Novel Model for Data Security and Integrity over Encrypted Cloud Data

In this section we will mainly discuss about proposed model for providing data security and integrity over the encrypted cloud data. Now let us discuss about this proposed model in detail as follows:

System Model

In this proposed system model, we mainly discuss about the various primitives that were used in our current thesis. For any cloud service provider, it contains three main entities like:

1. Data Owner,
2. Data User/Search User.
3. Cloud Server and

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) in encrypted form C = (C1, C2, . . . , Cn) to the cloud server and still preserve the search functionality on outsourced data. Here we assume that documents are labeled with D and if there are many documents to be out sourced they are represented as D1, D2 and so on. Here the documents what we take in our current paper consists of a general documents or text files and need to be stored in a secure manner inside a cloud server. Here the sensitive data is initially encrypted and then ready to store inside the cloud server, they are termed as C1, C2 and so as they were encrypted by the data owner at his level before out sourcing into the cloud server.

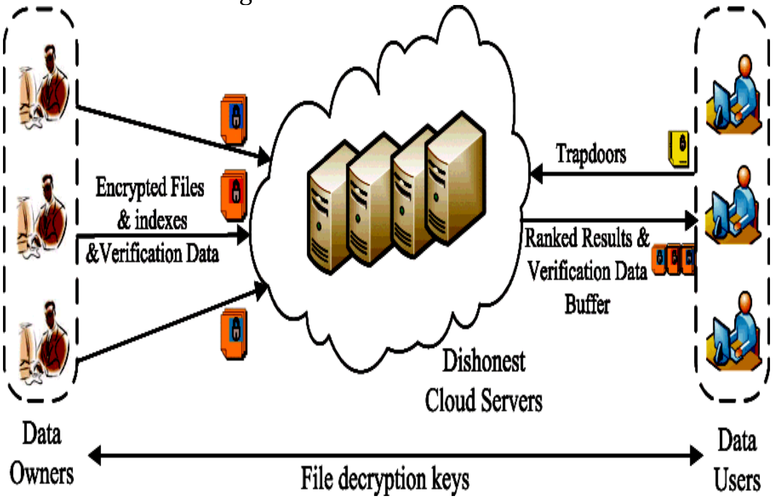

Figure.3. Represents the Proposed Model for Providing Security and Integrity over Encrypted Cloud Data

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. Now the data user try to search for the files and he try to request for the files from the cloud server and then he try to request for the decryption key for the data owner. Once the data owner sends the key, the data can be decrypted and view in a plain text manner.

IV. Implementation Phase

Implementation is a stage where the theoretical design is converted into programmatically manner. Here in this stage the application is mainly divided into several modules and each and every module differs from one another. In this proposed thesis, we try to divide the application into following four modules, they are as follows:

1) System Construction Module:

In this Module, we 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 each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption. We achieve the goal by constructing secure verification object for encrypted cloud data. Furthermore, a short signature technique with extremely small storage cost is proposed to guarantee the authenticity of verification object and a verification object request technique is presented to allow the query user to securely obtain the desired verification object. Performance evaluation shows that the proposed schemes are practical and efficient. Here we implement some modules they are Data Owner, Data User and Cloud Server.

2) Data Owner

In Data Owner module, Initially Data Owner must have to register their detail.After successful registration data owner can login and upload files into cloud server with encrypted keywords and hashing algorithms. He/she can view the files that are uploaded in cloud. Data Owner can approve or reject the file request sent by data users. After request approval data owner will send the trapdoor key and verification object through mail.

3) Data User

In Data User module, Initially Data Users must have to register their detail and after login he/she has to verify their login through secret key. Data Users can search all the files upload by data owners. He/she can send request to the files and then request will send to the data owners. If data owner approve the request then he/she will receive trapdoor, verification object and decryption key in registered mail

4) Cloud Server

In Cloud Server module, Cloud Provider can view all files details. Cloud can edit the files and update and also cloud server can view the download history

V.Conclusion

In this proposed thesis we finally implemented and analyzed 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 quality of each data file but also authorization of data by using MD5 Algorithm (message digest algorithm) in which the short signature key is generated and used for verifying the data authentication. By conducting various experiments on our proposed model, we finally came to a conclusion that our proposed approach is best in providing data integrity and security over sensitive data under the encrypted cloud data.

VI. References

1. S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in Proc.IEEE Conf. Comput. Commun., 2010, pp. 1–9.
2. S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Proc.14th Int. Conf. Financial CryptographyData Security, 2010, pp. 136–149.
3. D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Security Privacy,2000, pp. 44–55.
4. 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.
5. Y. Huang, D. Evans, J. Katz, and L. Malka, “Faster secure two party computation using garbled circuits,” in Proc. 20th USENIX Conf. Security Symp., 2011, p. 35.
6. C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation, Dept. Comput. Sci., Stanford Univ., Stanford, CA,USA, 2009.
7. Raul Isea The Present-Day Meaning Of The Word Bioinformatics, Global Journal of Advanced Research, 2015. 554-568, Apr. 2006.
8. P. Mell and T. Grance, “The nist definition of cloud computing,” http://dx.doi.org/10.602/NIST.SP.800-145.
9. K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.
10. S. Kamara and K. Lauter, “Cryptographic cloud storage,” in Springer RLCPS, January 2010.
11. D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in IEEE Symposiumon Security and Privacy, vol. 8, 2000, pp. 44–55.
12. E.-J.Goh, “Secure indexes,” IACR ePrint Cryptography Archive, http://eprint.iacr.org/2003/216, Tech. Rep., 2003.
13. D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Public-key encryption with keyword search,” in EUROCRYPR, 2004, pp. 506–522.