*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. III (Mar – Apr. 2015), PP 63-66*
*www.iosrjournals.org*

# Secure Data Storage in Cloud Using Encryption and Steganography

Akhil S Killawala[1], Kaustubh R Kulkarni[2], Nishant D Gohel[3],
*1,2,3 Dept. of Computer EngineeringK J Somaiya College Of Engineering,Mumbai-77,Maharashtra,India*

***Abstract:*** *In this project, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible scheme combining cryptography and steganography. Encryption module encrypts the files before they are uploaded and decryption module decrypts them when they are downloaded. The text steganography inserts a watermark within an html file to uniquely identify it's owner. The image steganography embeds the watermark within an image file.*

***Index Terms:*** *Secure Storage, Cloud, Encryption, Text Steganography, Image Steganography.*

## I. Introduction

Cloud computing has been envisioned as the next generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges.

In this project, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible scheme combining cryptography and steganography Encryption module encrypts the files before they are uploaded and decryption module decrypts them when they are downloaded. The text steganography inserts a watermark within an html file to uniquely identify it's owner . The image steganography embeds the watermark within an image file. The project also has authentication and access control features, for example, blocking a particular suspicious IP address. All malicious attempts to access the system are logged for future reference. Mobile alerts module has also been incorporated on an experimental level to simulate an attacker so that, thus alerted , the owner can take appropriate steps like blocking that IP address etc.

## II. Existing System

From the perspective of data security, which has always been an important aspect of quality of service, Cloud Computing inevitably poses new challenging security threats for number of reasons. Firstly, traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing. Therefore, verification of correct data storage in the cloud must be conducted without explicit knowledge of the whole data. Considering various kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc. To ensure storage correctness under dynamic data update is hence of paramount importance. These techniques, while can be useful to ensure the storage correctness without having users possessing data, cannot address all the security threats in cloud data storage, since they are all focusing on single server scenario and most of them do not consider dynamic data operations. As an complementary approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers. Again, none of these distributed schemes is aware of dynamic data operations. As a result, their applicability in cloud data storage can be drastically limited.

## III. Problem Definition

Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy.

This unique attribute poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. We have to ensure the correctness of users' data in the cloud as well.

## IV. Proposed System

In this paper, we propose an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud.

Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of data error.

The proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack and server colluding attacks

To ensure the correctness of users' data in the cloud, we propose an effective and flexible scheme combining cryptography and steganography.

Encryption module encrypts the files before they are uploaded and decryption module decrypts them when they are downloaded. The text steganography inserts a watermark within an html file to uniquely identify it's owner . The image steganography embeds the watermark within an image file. The project also has authentication and access control features, for example, blocking a particular suspicious IP address. All malicious attempts to access the system are logged.

## V. Modules

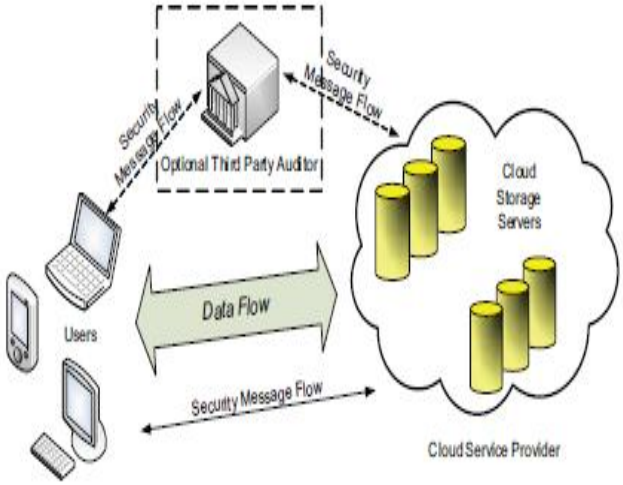


**Fig 1:** Interaction Of Modules

**Client Module:**

In this module, the client sends the query to the server. Based on the query the server sends the corresponding file to the client. Before this process, the client authorization step is involved.In the server side, it checks the client name and its password for security process. If it is satisfied and then received the queries form the client and search the corresponding files in the database. Finally, find that file and send to the client. If the server finds the intruder means, it set the alternative Path to those intruder.

**System Module:**

Representative network architecture for cloud data storage is illustrated in Figure 1. Three different network entities can be identified as follows:

- User:
- Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.
- Cloud Service Provider (CSP):
- A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems,.
- Third Party Auditor (TPA):

An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

**Cloud data storage Module:**

Cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a simultaneous, the user interacts with the cloud servers via CSP to access or retrieve his data. In some cases, the user may need to perform block level operations on his data.. users should be equipped with security means so that they can make continuous correctness assurance of their stored data even without the existence of local copies. In case that users do not necessarily have the time, feasibility or resources to monitor their data, they can delegate the tasks to an optional trusted TPA of their respective choices. In our model, we assume that the point-to-point communication channels between each cloud server and the user is authenticated and reliable, which can be achieved in practice with little overhead.

**Cloud Authentication Server:**

The Authentication Server (AS) functions as any AS would with a few additional behaviors added to the typical client-authentication protocol. The first addition is the sending of the client authentication information to the masquerading router. The AS in this model also functions as a ticketing authority, controlling permissions on the application network. The other optional function that should be supported by the AS is the updating of client lists, causing a reduction in authentication time or even the removal of the client as a valid client depending upon the request

**Unauthorized data modification and corruption module:**

One of the key issues is to effectively detect any unauthorized data modification and corruption, possibly due to server compromise and/or random Byzantine failures. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data error lies in is also of great significance

**Adversary Module:**

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, untrusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for monetary reasons, but it may also attempt to hide a data loss incident due to management errors, Byzantine failures and so on.

On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period. Specifically, we consider two types of adversary with different levels of capability in this paper:

Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is comprised, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

**Encryption Module:** Provides only essential encryption using Rijndael algorithm.

**Text Steganography Module:**

Hides watermark as binary data within an HTML file by considering order of attributes within tags to denote a 1 or a 0.

**Image Steganography Module:**

It uses LSB steganography. In RGB color model Red is represented by one byte, Blue by one byte and Green by One byte. The mechanism replaces 4 LSBs of every byte with watermark information to be propagated through the image.

.

## VI. System Requirements

Hardware Requirements:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive: 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

Software Requirements:

- Operating system : - Windows XP.
- Coding Language :-JAVA,Swing,RMI,J2me(WirelessToolkit)
- Tool Used: - Eclipse 4.3

## VII. Conclusion

- Cloud computing extend beyond a single company or enterprise.
- To ensure the correctness of users' data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append.
- We believe that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and many research problems are yet to be identified

## Acknowledgment

We wish to express true sense of gratitude towards our guides Prof. Deepak Sharma and Prof. Sheetal Pereira for their constant encouragement and valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project. We would like to thank our Head of Department Prof. Bharathi H N & all staff members who extended their kind support during the accomplishment of the project. Finally, we express my sincere thanks to all those who helped us directly & indirectly in many ways in completion of this project.

## References

[1]. Patidar Shyam,Rane Dheeraj,Jain Pritesh,A Survey Paper on Cloud Computing, Second International Conference on Advanced Computing & Communication Technologies (ACCT),7-8 Jan 2012

[2]. Wojciech Mazurczyk, Krzysztof Szczypiorski, Is Cloud Computing Steganography-proof?,Third International Conference on Multimedia Information Networking and Security,2011

[3]. Krešimir Popović, Željko Hocenski, Cloud computing security issues and challenges, MIPRO 2010, May 24-28, 2010, Opatija, Croatia

[4]. Atallah M. Al-Shatnawi,A New Method in Image Steganography with Improved Image Quality, Applied Mathematical Sciences, Vol. 6 no. 79, 3907 – 3915, 2012

[5]. Souvik Roy, P.Venkateswaran, A Text based Steganography Technique with Indian Root, International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

[6]. Rafat, K.F. , Enhanced text steganography in SMS, Computer, Control and Communication, 2009. IC4 2009. 2nd International Conference on , 17-18 Feb. 2009

[7]. Shirali-Shahreza, M. , Shirali-Shahreza, M.H., Text Steganography in SMS, Convergence Information Technology, 2007. International Conference on , 21-23 Nov. 2007

[8]. Andreas Westfeld, F5—A Steganographic Algorithm,Information Hiding - 14th International Conference, IH 2012, Berkeley, CA, USA, May 15-18, 2012

[9]. Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, "Ensuring data storage security in Cloud Computing," Quality of Service, 2009. IWQoS. 17th International Workshop on , vol., no., pp.1,9, 13-15 July 2009