International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-4, April 2015

Data Integrity Proofs in Online Storage

Prof. Rahul Sathawane, Akash Thakre, Kalyani Dhakate, Sushant Waghmare

***Abstract*— Data integrity is a fundamental aspect of storage, security and reliability. With the advent of network storage and new technology trends that result in new failure modes for storage, interesting challenges arise in ensuring data integrity. Online storage has been envisioned as the ultimate solution to the rising storage and access need of every person and IT Enterprises. With the high costs of data storage devices as well as the rapid rate at which data is being generated it proves costly for enterprises or individual users to frequently update their hardware. Apart from reduction in online storage costs, it also helps in reducing the maintenance. Online storage moves the user's data to large data centres, which are remotely located, on which user does not have any control. However, this unique feature of the cloud poses many new security challenges which need to be clearly understood and resolved. We provide a scheme which gives a proof of data integrity in the online storage which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the services provider and the customer and can be incorporated in the Service level agreement (SLA).**

One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in Online Storage. In this project we provide a scheme which gives a proof of data integrity in Online Storage which the customer can employ to check the correctness of his data in the storages. The user can have the proof of the integrity of the data uploaded by him on the Web Storage

***Index Terms*—Data Integrity, Cloud**

I. INTRODUCTION

Data outsourcing to web storages servers is raising trend among many firms and users owing to its economic advantages. This essentially means that the owner (client) of the data moves its data to a third party storage server which is supposed to - presumably for a fee - faithfully store the data with it and provide it back to the owner whenever required.

As data generation is far outpacing data storage it proves costly for small firms to frequently update their hardware whenever additional data is created. Also maintaining the storages can be a difficult task. Storage outsourcing of data to web storage helps such firms by reducing the costs of storage, maintenance and personnel. It can also assure a reliable storage of important data by keeping multiple copies of the data thereby reducing the chance of losing data by hardware failures. Storing of user data on online storage, despite its advantages has many interesting security concerns which need to be extensively investigated for making it a reliable solution to the problem of avoiding local storage of data. In this paper we deal with the problem of implementing a protocol for obtaining a proof of data possession on online storage, sometimes referred to as Proof of retrievability (POR). This problem tries to obtain and verify a proof that the data that is stored by a user at a remote data storage in the web/online (called web/online storage archives or simply archives) is not modified by the archive and thereby the integrity of the data is assured. Such verification systems prevent the web/online storage archives from misrepresenting or modifying the data stored at it without the consent of the data owner by using frequent checks on the storage archives. Such checks must allow the data owner to efficiently, frequently, quickly and securely verify that the web/online archive is not cheating the owner. Cheating, in this context, means that the storage archive might delete some of the data or may modify some of the data.

II. METHODOLOGY

Storing of user data on the online storage despite its advantages has many interesting security concerns which need to be extensively investigated for making it a reliable solution to the problem of avoiding local storage of data. Many problems like data authentication and integrity (i.e., how to efficiently and securely data is stored) also ensuring that the online storage server returns correct and complete results in response to its clients' queries.

The user need a way to know the integrity of the file and data that is stored on the online storage. And also to ensure the security of the that data. One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data on the storage. As the data is physically not accessible to the user the online storage should provide a way for the user to check if the integrity of his data is maintained or is compromised. In this project we provide a scheme which gives a proof of data integrity on the online storage which the customer can employ to check the correctness of his data. This proof can be agreed upon by both the service provider and the customer and can be incorporated in the Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

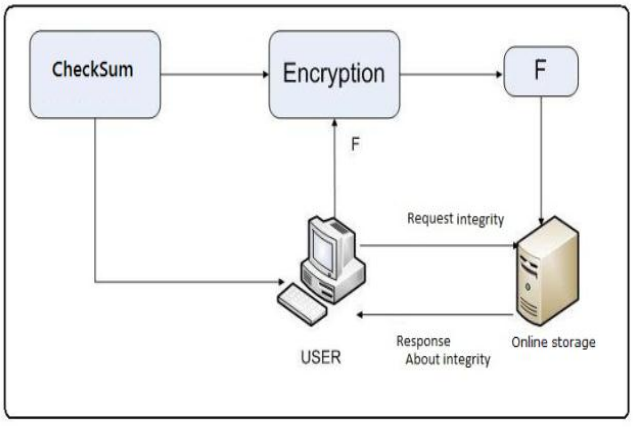

Fig1.Data Flow Diagram For Structure of Storage

The first we have checked is previously used algorithms like RSA, public key cryptography algorithms etc, but the problem with these techniques are, they can be used only on textual files or images. If we apply these algorithms on executable files, then that files gets corrupted. So the first option is not suitable for the entire files which may be uploaded on the online storage. The second method which was tested is hash check method, like MD5, SHA. In this technique we need to upload file as it is, and the hash value of the file is stored in the file data base. The second method which was tested is hash check method, like MD5, SHA. In this technique we need to upload file as it is, and the hash value of the file is stored in the file data base

III. RESULTS & DESCUSSIONS

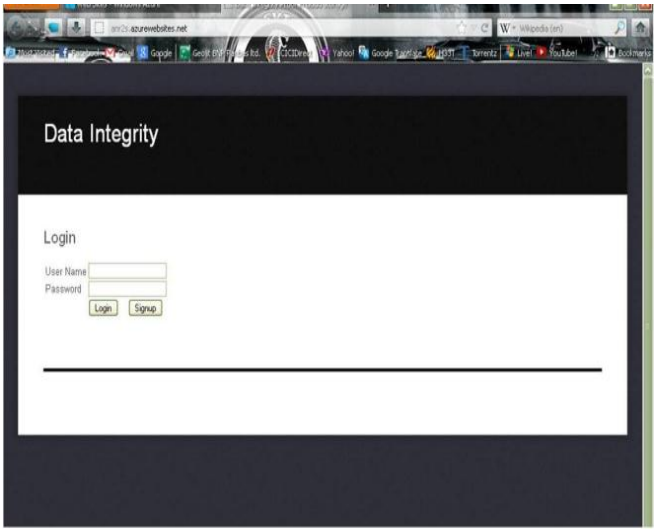

Fig2. Login Page

The user will have to login to get access for the website. The username and password set will be entered in the login box. After logging in, the home screen will appear.

- Login with credentials created while sign up.
- Upload file on web site.
- User can view the file.
- User can edit the file (text files).
- Delete file online storage.

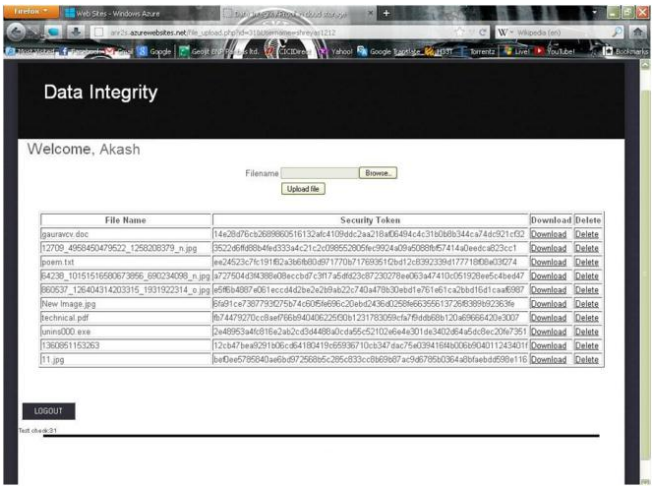

Fig3. Uploaded files and their Security Token

This is screen shows the user information about the uploaded files. Here the file is decrypted

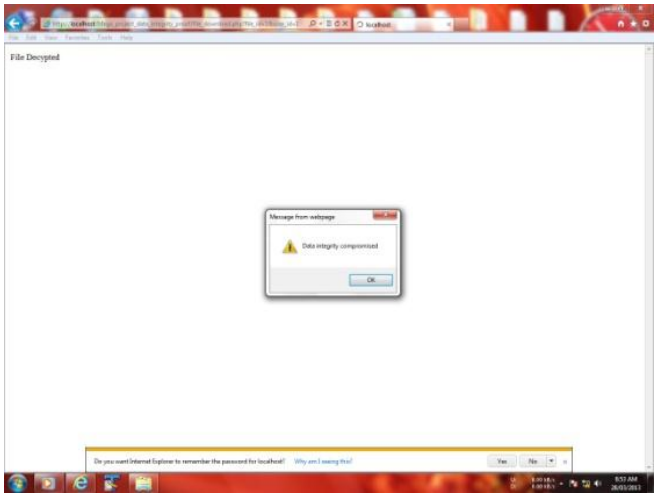

Fig4. Manipulation in files.

Here the file is decrypted, if a not authorised user tries to access the database the file will not be decrypted and it is decrypted somehow it will show the above message

IV. CONCLUSIONS

In this paper we have worked to facilitate the client in getting a proof of integrity of the data which he wishes to store in the storage servers with bare minimum costs and efforts.
As such there are no disadvantages in our project, but in future if anyone could find it out, we'll be happy to learn from them.

REFERENCES

[1].Cryptography and Network security by William stallings.
[2]. Programming PHP By- Rasmus Lerdorf, Kevin Tatroe
[3].Data Integrity Proofs in Cloud Storage by Sravan Kumar R & Ashutosh Saxena, , India, IEEE paper 2011