



Improving Data Integrity for Storage & Recovery Security in Cloud Computing

Prof. Ashwini Mandale¹, Pradnyarani Chavan²

Professor, CSE, DACOE, Karad, India¹

Student, CSE, DACOE, Karad, India²

Abstract: The cloud computing has been developed as the next generation architecture in IT industry. In addition to traditional solutions where IT services are under control of physical/ logical/ personal controls. Cloud computing moves to the application software as well as databases to the large data centres, where large amount of data and services manage properly. These maybe not fully trusted. So, that causes to introducing new challenges in cloud era. In this paper we are focusing on Cloud Security, Data Integrity, authentication, authorization. Here basically storage correctness, fast localization, dynamic data support, dependability are take into consideration.

Keywords: Cloud Computing, Cloud Service Provider, Cloud Security Services, Data Integrity, Data Recovery, Third Party Auditor.

I. INTRODUCTION

Cloud computing becomes more popular in recently, also it provides storing data of various types on the cloud servers or cloud storage. Basically cloud computing is the network driven technology. Cloud storage acts as pool between hardware resources and software resources present on local computer and server computer. Cloud computing as a new generation Technology promises to achieve the need of security for storing and accessing data on cloud. Cloud is highly scalable and provides infinite computing services and resources as per user needed at any time. All the resources are available at any corner of world. All the resources are highly scalable and integrated on environment. Cloud computing resources are provided by internet. Online storage can eliminate overhead of storing and accessing data on local machine. Cloud provides number of benefits such as flexibility, integrity and pay as per use of basis. The major problem of data security is crucial part when the data is confidential.

However maintaining security is a challenging task. There exist many systems to solve the problem of data integrity. The auditing can be performed in two ways private and public. Public audit ability is more convenient and preferred than private. In some situation if data is lost then it is available on cloud service provider (CSP). Traditional cryptographic primitives for the purpose of data security protection cannot 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. 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. In this paper, we used models which are shared data on different computer devices by executing system models on IIS base. For that purpose we are uses the OTP (One Time Password) system. This will be also helpful for the better security purpose.

The main aim of this paper is:

The challenge in our work further provides localization of Data Error.

- We propose Efficient Method for Data Encoding stored in cloud.
- We propose Efficient Method for Data Recovery in case of data lost.
- To Achieve public and private auditability and for Detecting Third Party (hacker) who achieve the data and also block that hacker.

II. RELATED WORK

Cloud computing is basically a system which consist of some basic entities that as follows,

1] Client (User):

A client or user is the entity of network whose store the data on to the cloud and depend on that cloud for maintenance of that data.

2] Cloud Service Provider (CSP):

CSP is the one kind of server of cloud that provides sufficient space for storage, various resources and maintenance for the client or user data.

There are various services that are used in to the cloud computing,



- Software as a Service (SaaS): Including number of software.
- Platform as a Service (PaaS): For developing or hosting applications use computing Platforms.
- Infrastructure as a Service (IaaS): Use of computing infrastructure or entire networking.

3] **Third Party Auditor (TPA):**

TPA is that the outsider evaluator who might review those majority of the data for information manager or consumer so it will absolve the load from claiming management from claiming learning of information manager.

For Data Security, Data Integrity, recovery of data reason we provide the system of blocking an unauthorized user by using its IP address. Also we gave the privacy for that data with the help of creating private cloud and public cloud in the cloud storage system. For the detecting error into the data added by the client/user we apply some basic algorithms such as

- Token Pre-computation
- Correctness Verification and Error Localization
- Error Recovery

III. PROBLEM STATEMENT

Cloud computing is the data structure used for the storing the data. But the main problem is occurred when the unauthorized user can try to access or hack that data. So, for the security reason and providing proper access to proper user is one of the difficult tasks. Also avoid the fraudulent changes done by the unauthorized user into the original data. Into the cloud there are storage of abundant sized data due to that the redundancy may occurs into the user's cloud storage. And if the any user accessed his data for no longer time then the proper techniques for maintenance of that data.

IV. PROPOSED SYSTEM

The problems which are stated into the problem statement that are try to resolve in this paper. For that purpose some models we are used here that are listed below.

1. Storage Correctness
2. Fast Localization
3. Dynamic Data Support
4. Dependability

Basically, these models are nothing but the way of the reducing rate of the difficulties occurs into the cloud when user going to use it. These models are explained as follows,

1. Storage Correctness:

- To ensure user that their data are indeed stored appropriately and kept in intact all the time in the cloud.
- Cloud Storage should have more accurate data.
- The data stored in cloud is provided by the authenticated user.
- So, the data could be of any type like audio, video, JPG, PDF, text.
- It fully depends on the authorized user who has the access to cloud storage.
- They can store the data whatever they want.
- To access that cloud data user should have to login with their proper password.
- Cloud storage gives data which is available in the cloud and related data to the user.

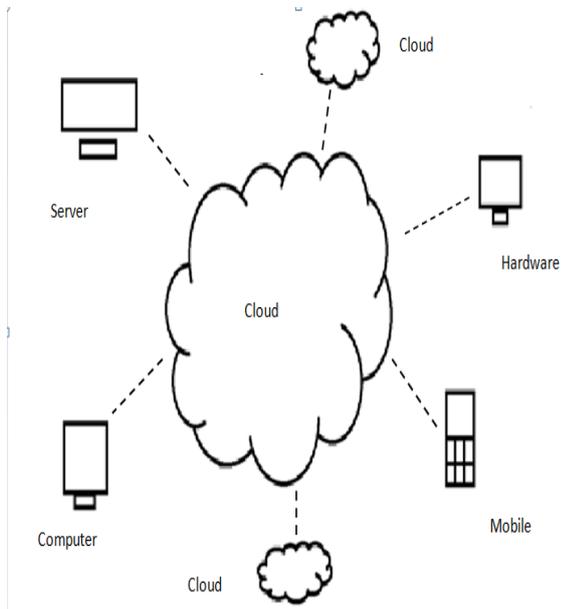


Fig.1. Cloud Network

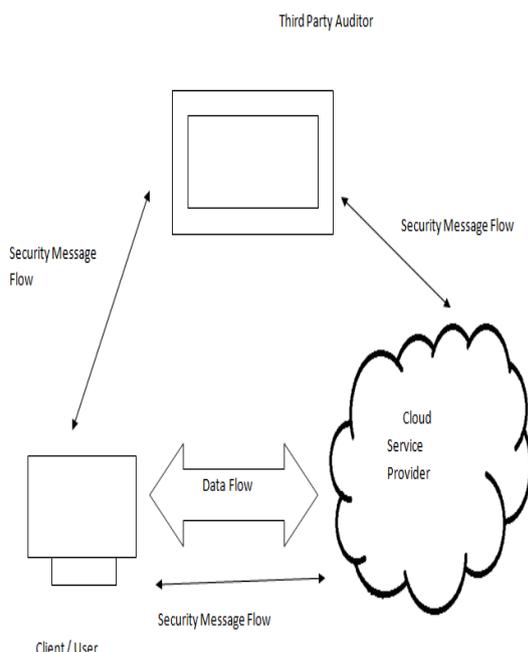


Fig.2. Cloud Data Storage Architecture



2. Fast Localization:

- When the data corruption has been detected then the malfunctioning server located effectively.
- The fast localization while transferring data from cloud to local and any error occurred then error correction performed.
- While transferring data and any other file, it will get corrupted then automatically it will repair.
- The error recovery is fast then availability of data rate is automatically high.

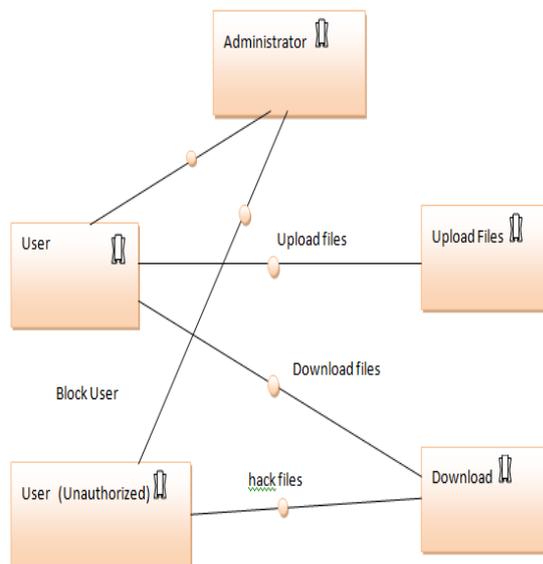


Fig.3. System Design

3. Dynamic Data Support:

- Cloud contains the storage of various kinds of data that can be any time added or deleted by the user.
- So, cloud has to provide dynamic data support to the user data.
- In that the main point is the when the user make changes into his data then that changes must have to apply on the data which stored on to cloud.
- The dynamic changes may contain the deletion, updating, and modification into data.
- The cloud has responsibility to available that modified data to user very fast and correctly without done any error.
- It also contains the management of data to the proper way and provides assurance of data to the user.

4. Dependability:

- Cloud has to maintain the dependence of data stored on the cloud after the happening of unwanted changes occurred in data.
- Also, the data availability after the malicious data modification and server colluding attacks.
- Cloud has to minimize the effect done by the data errors or failure of server.
- It has to enhance the proper availability as well as the correct data.

V. CONCLUSION

In this paper, we focused on data security, data integrity, also the availability of data on cloud storage. Data integrity plays important role in cloud computing for security purpose. We propose a model based on secure data possession in multi-cloud model. The private key generator is used in our model which produce a private key (One Time Password) for unique identity of user/client. We discussed here Storage Correctness, Fast Localization, Dynamic Data Support, Dependability techniques for improving data security and integrity of data also proper utilization of storage on the cloud. We provide a better way to security of data by preventing the security attacks done on the cloud data.

ACKNOWLEDGEMENT

We like to acknowledge our gratitude to Prof. A. N. Mandale for valuable suggestions in carrying our research work. We also thankful to CSE department of our college.

REFERENCES

- [1] Cong Wang, Qian Wang, and KuiRen, "Ensuring Data Storage Security in Cloud Computing", July 2011.
- [2] RampalSingh, SawanKumar, ShaniKumarAgrahari, "Ensuring Data Security in Cloud Computing", March 2013.
- [3] Poonam M. Pardeshi, "Improving Data Integrity for Data Storage Security in Cloud Computing", June 2015.
- [4] N. Gohring, "Amazon's S3 down for several hours", "online at http://www.pcworld.com/businesscenter/article/142549/amazons_s3_down_for_several_hours.html, 2008.
- [5] A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.
- [6] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. of Asiacrpts '08, Dec. 2008. Web Site: www.Google.com