Data Security in Private Clouds using Erasure Correcting Code

B.Dhivya[1], N.Geethanjali[2] ,R. Priyadharshini[3]
[1,2,3]*Department of Information Technology, SNS College of Technology, India.*

Abstract

Cloud Computing is a computing model which became the largest buzzword in the IT world. Cloud can be used based on an "on-demand" scenario. The user can access the resources in the cloud and pay for what they have used. Hence cloud is a "pay per use" service. Cloud enables user to outsource their data and hence user can be free from physical management of data which traditionally has been expected by both enterprises and individuals with high service-level requirements. Although they provide more advantages still there exist threats towards ensuring the data integrity and availability. Inorder to ensure data integrity the proposed system utilizes erasure correcting code for its file distribution and verification among the distributed cloud sever(s).The proposed system also enables simultaneous identification of the misbehaving server and prevents from malicious data modification attack. The data stored in the cloud are most often modified and updated the system is further extended to support the dynamic operations like insert, delete, append over the user data file.

1. Introduction

In the cloud computing model "customers" plug into the "cloud" to access IT resources which are prices and provided "on-demand". Economically, the main appeal of cloud computing is that customers only use what they need, and only pay for what they actually use. Resources are available to be accessed from the cloud at any time, and from any location via the internet. The customers need not worry about how things are being maintained behind the scenes – the customers simply purchase the IT service they require as like any other utility. Because of this, cloud computing has also been called utility computing, or 'IT on demand'[2].

One fundamental aspect of the cloud computing model is that data is being centralized or outsourced into the cloud. Cloud storage vendors use massive data centers to store vast amounts of data, storing not Terabytes of data but Petabytes in some cases (one quadrillion bytes, or 1000 terabytes).From the user's perspective, including both individuals and IT enterprises, storing data remotely in a cloud is a flexible on-demand manner brings appealing benefits[2].

While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats to the outsourced data. Since Cloud Service Providers(CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data[3]-[5]. As a result, the correctness of the data in the cloud is put at risk due to the reasons like internal and external threats to data integrity, outages and security breaches. These threats in cloud services may appear from time to time. Amazon S3's recent downtime[6], Gmail's mass deletion[7] incident, and Apple Mobile Me's post-launch downtime are all such examples.

In order to provide security and to achieve the assurances of cloud data integrity and availability and to enforce the quality of cloud storage service, efficient methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. Erasure Correcting Code is a forward error correction code which is one of the efficient methods to ensure the data integrity of the users data and to simultaneously identify the misbehaving server available in the cloud. It also enables user to perform dynamic operations over the outsourced data.

2. Security System in Cloud

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.

- Traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted due to the users' loss of 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 ware house. 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[8].

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 v focusing on single server scenario and most of them donot consider dynamic data operations.

2.1 Problem Statement

Some kinds of threats towards the cloud data integrity is still available. Because cloud data donot reside at user's local site but at CSP's address domain, these threats can come from two different sources: internal and external attacks. For internal attacks, 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 errors, Byzantine failures and so on. [3]For external attacks, data integrity threats may come from outsiders who are beyond the control domain of CSP, for example, the economically motivated attackers.[5] They may compromise a number of cloud data storage servers in different time intervals and subsequently be able to modify or delete user's data while remaining undetected by CSP.

3. Security using Erasure Correcting Code

The system must be able to provide data integrity and provide security to the user data file against threats that are imposed. Erasure Correcting Code is used for file distribution and verification of the user data in in the cloud storage system[9]. The ip address of the server can be used to access the user data file. The user will be allowed to access the user data file only when they access through the valid server ip address. The user can also include restricted ip address at the cloud server site. The auditing process enables to make the correctness verification along with the simultaneous identification of the misbehaving server(s). The cloud server can be designed to have the details about the hackers who are trying to make an attempt to access the user data file. The system allows the user to perform the dynamic operation over the data that are stored at the server site only when they access from the valid server ip address. The system flow diagram fig1 explains the overall working of the system.

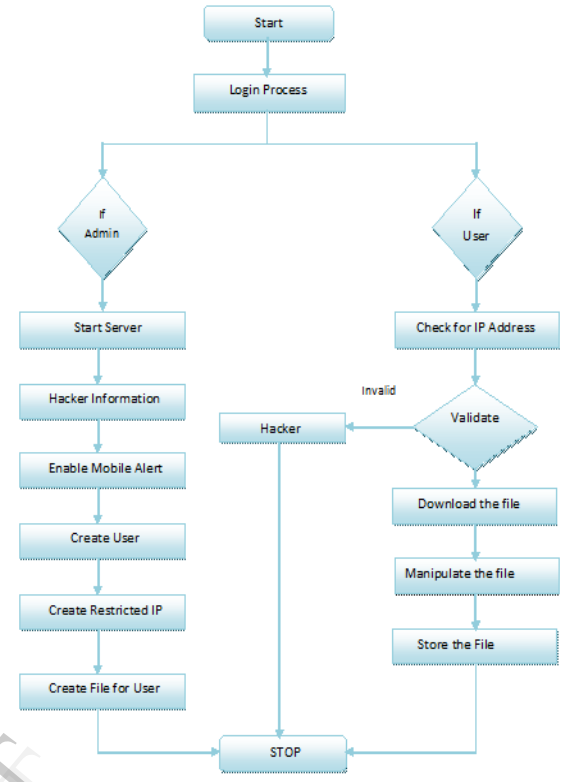

Fig1. System flow diagram

The user can create their account at the cloud server site. They can create their data file at the server site. At the time of creation the user need to specify the allowed server ip(fig 2) address from which the user can access the data file. The user data file will be created at the cloud server site which is displayed at the available resources pane (fig 3). The user can also provide the restricted ip address (fig 3)

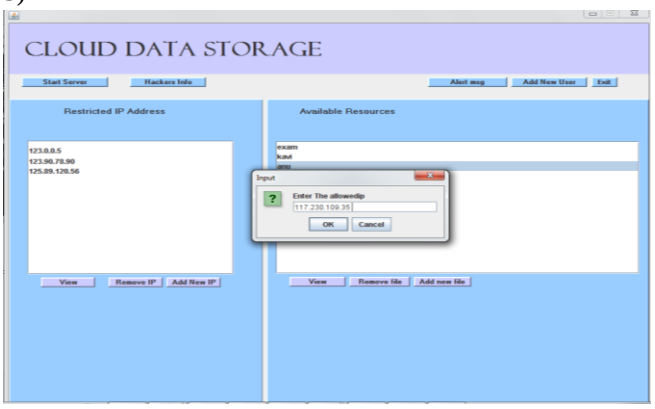

Fig 2. User providing allowed ip address

Fig 3.User creating file at cloud server site

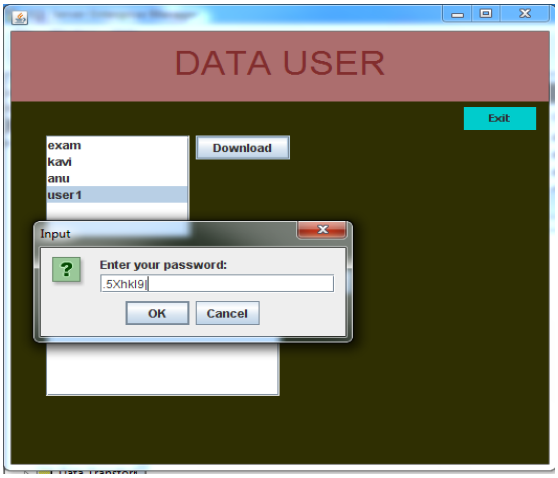

Fig4b.Attempt to user1file from invalid ip

Fig 4a. Shows the user makes a valid attempt to access the user1 data file. The user can perform the dynamic operations over the user1 file.

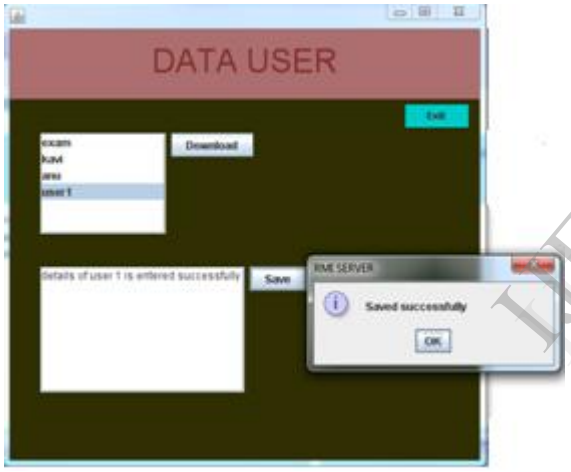

Fig 4a. Attempt to user1 file from valid ip

If anyone tries to access the user1 file from another ip address they will not be allowed to access the file. Instead they will be requested to provide their password (fig 4b). Their attempt will be considered as a hacking attempt. The hackers will be intimated as they have committed some mistake while providing password. This attempt will be sent as an alert message to the user mobile as in fig5. It will contain the hacker name and the ip address from which the hacking attempt is made. The history of the hacking attempt will also be stored at the cloud server site (fig 6).It will contain the entire details about the hacker. The information may include hacker name, ip address from which they have made an attempt, the file name to which they have made the attempt and the time at which they made the attempt.

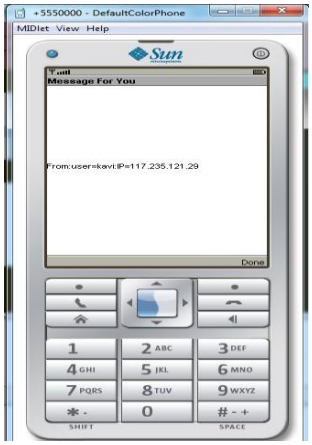

Fig5. Hacking attempt alert message

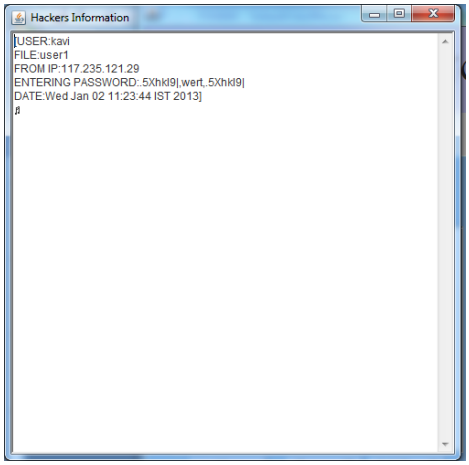

Fig6. Hackers information log at server site

Design goals of the system

The system tends to provide the following properties:

- Storage correctness
- Fast localization of data error
- Dynamic data support

4. Conclusion

The problem of data security in cloud data storage is investigated which is essentially a distributed storage system. To ensure the correctness of user's data in cloud data storage, an effective and flexible distributed scheme with explicit dynamic data support including block update, delete, and append is to be designed. Erasure Correcting Code can be used in the file distribution preparation to provide data in the cloud server. The system increases the availability of the data file. The usage of the erasure correcting code achieves the integration of storage correctness insurance and data error localization, i.e., whenever data corruption has been detected during the storage correctness verification across the distributed servers, we can almost guarantee the simultaneous identification of the misbehaving server(s). The detailed security and performance analysis shows that the system is highly efficient and resilient to malicious data modification attack.

5.References

[1]David Buford, CFA, MBA, MCP,"Cloud Computing: A Breif Introduction",www.ladenterprizes.com
[2]David X" Assessing Cloud Node Security", March 2011, www.contextis.com
[3]J.KinCaid, "MediaMax/TheLinkup Closes Its Doors," Online at http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-close-its-doors/, July 2008.
[4]S.Wilson, "Appengine outage," Online at http://www.cio-weblog.com/50226711/appengine_outage.php, June 2008.
[5]B.Kerbs, "Payment Processor Breah May be Largest Ever,",Online at http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breah_may_b.html, Jan. 2009.
[6]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
[7]M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/, December2006.
[8]G.Ateniese, R. Burns, R.Curtmola, J.Herring, L.Kissner, Z.Peterson, and D.Song, "Provable data possession at untrusted stores," in Proc. Of CCs'07, Alexandria, VA, October 2007,pp.598-609
[9]C.Wang, Q.Wang, K.Ren, and W.Lou,"Ensuring data storage security in cloud computing," in Proc of IWQos'09, July 2009, pp.1-9