ISSN:0975-9646

Secured Data Sharing in the Cloud

Amrut Hunashyal
B.V.B CET
Hubli,India.

Chetak Patil
B.V.B CET
Hubli,India.

Vilas Balaganur
B.V.B CET
Hubli,India.

Abstract- Cloud computing will play a major role in the future internet of services and it has opened up new challenges by introducing different types of trust scenarios. An important characteristic of the cloud services is that the user's data are accessed on demand provisioning of applications, platforms, and computing infrastructures it can become a roadblock to the wide usage of cloud services around the globe. This paper presents a framework for distributed accountability and auditing which is used to protect user's data and also monitor the actual usage of data in the cloud. In particular, we propose a security mechanism which will keep track usage of data in the cloud. Apart from that we are going to increase the security of user's data by the encryption of data files and also using a security prototype, 'Something you know and something you have'. We provide experimental studies that illustrate the efficiency of the proposed.

Keywords- Cloud computing, data sharing, security, something you know and something you have.

I. INTRODUCTION

Cloud computing technology is flexible, highly scalable and gives us technology-enable services that can be easily consumed over the Internet on as-needed basis. Cloud computing technology allows cloud servers to reside anywhere, thus the enterprise may not know the physical location of the server used to store and process their data and applications. Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services.

It is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud. Data owner should not bother about his data, and should not get fear about damage of his data by hacker, there is need of security mechanism which will keep track usage of data in the cloud. It also provides reliable information about usage of data and it observes all the records, so it helps in make trust, relationship.

In this paper we have used 'something you have and something you know' authentication method. In this, while registering into the cloud, Data owner needs to provide the USB device (pen drive) details along with username and password. Whenever Data owner wants to access to the cloud he needs to insert the device and has to enter the username and password for verification. This approach will help the data owner to login securely into the cloud. Even if his password is hacked then no one can access data into his cloud without his USB device hence Man in the Middle attack is restricted.

In our Framework for accountability and accounting first the data owner will set the policies for the data which he/she wants to place in cloud and send it to cloud service provider (CSP), any access to the data will be automatically check Distributed Accountability and Auditing in Cloud for its authentication and logs the record for each data item accessed and sent to data owner for monitoring the data usage and authenticity of the user.

II. RELATED WORK

In this section we review some related works concerned with security and privacy issues in cloud. Also, we briefly discuss the work which adopt similar techniques as our approach but serve for different purposes

Security and Privacy issues in cloud

Data resting in the cloud needs to be accessible only by those authorized to do so, making it critical to both restrict and monitor who will be accessing the data through the cloud. In order to ensure the integrity of user authentication, need of security mechanism which will keep track usage of data in the cloud users are accessing the data. As with all cloud computing security challenges, it's the responsibility of the user to ensure that the cloud provider has taken all necessary security measures to protect the user's data and the access to that data. Till today, little work has been done regarding accountability and auditing in cloud and lot to be researched. A proposed accountability mechanism to address privacy concerns of end users and user's private data are sent to the cloud in an encrypted form and the processing is done on the encrypted data.

III. OVERVIEW OF OUR PROPOSED WORK

In this section we have explained the components in detail.

A. Cloud Information Accountability (CIA):

In this section, we present an overview of the Cloud Information Accountability framework and discuss how the CIA framework meets the design requirements discussed in the previous section. The Cloud Information Accountability framework proposed in this work conducts automated logging and distributed auditing of relevant access

performed by any entity, carried out at any point of time at any cloud service provider.

B. Logger:

Finally, the data owner will be alert with the automatically generated log files about their data usage using two auditing modes such as push and pull mode. In the push mode the owner will be triggered automatically with the log files. Using this mode owner can ensure the size of the log record and timely detection of the user access. In the Pull mode the data owner are allowed to request to retrieve the logs at anytime when they want to check the recent access of their data items.

C. Authentication Technique

In this we have used something you have authentication method. In this, while registering into the cloud Data owner needs to provide the pen drive details along with username and password. Whenever Data owner wants to access to the cloud he needs to insert the pen drive and has to enter the username and password for verification. USB device's serial number will be saved into the database and will be verified with every time the user and owner is trying to log in.

D. User Interface Design

In this phase we create a GUI page, which acts as a median to connect the user with the cloud and through which user can able to send request to the cloud, by mean time cloud server can send the response to the user. In other words, this phase establishes the communication between the user and the cloud. So with this GUI page user can able to know about the overview of the whole application.

Fig.(a). Overview of the proposed system.

MODULES:

The major buildings modules of proposed systems are Four. They are.

1. DATA OWNER MODULE
2. CLOUD SERVICE PROVIDER MODULE
3. LOG GENERATOR
4. OPENSTACK PRIVATE CLOUD

1. Data Owner Module:

In this module, the data owner uploads their data in the cloud server. The new users can register with the service provider and create a new account and so they can securely upload the files and store it. The data owner can set the access privilege to the data file. To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud.

2. Cloud Service Provider Module

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud. To access the shared data files, data consumers download data files of their interest from the cloud.

3. Log Generator

Data owner will be alert with the automatically generated log files about their data usage. The Data owner will be triggered automatically with the log file whenever the user downloads the file.

4. OpenStack Private Cloud

We have used The Open Stack Cloud platform for setting the cloud. It is open source software for building private cloud. Predominantly acting as an infrastructure as a service. Platform, it is free and open-source software.

IV. PERFORMANCE STUDY

In this section, first we discuss the implementation of our concept and then analyze the security issues.

A. Implementation

Here we have developed our framework in PHP platform and for cloud storage we have used Open stack. We tested the framework by uploading and downloading the files.

Few snapshots of our framework

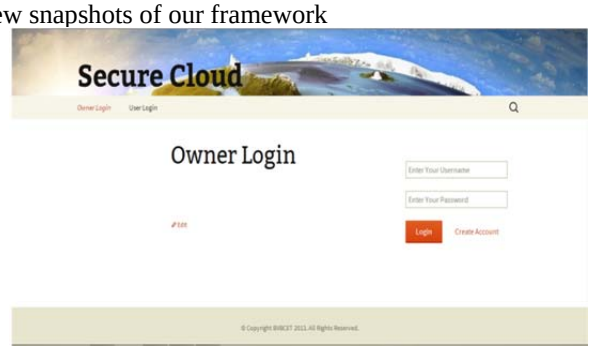

Fig (a): Login page of our framework

The fig (a) shows the view of login page of our Framework. The logging mechanism consists of user name and password.

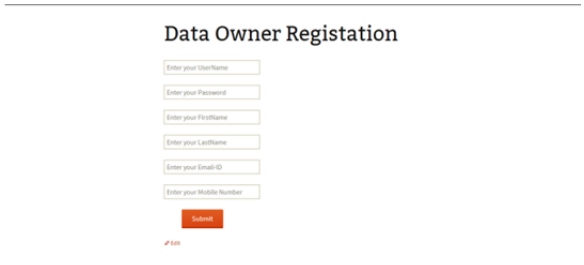

fig (b): Registration form

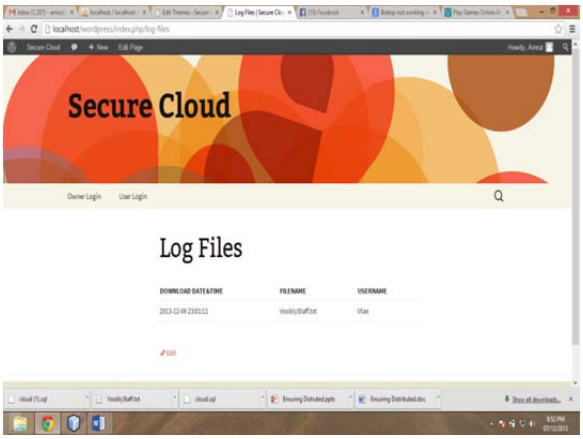

fig (c): Log Generation form

B. Security Study

In this section let's analyze some possible attacks on our framework.

1. Unauthorized user:

If some unauthorized person tries to access the data, first of all it is impossible as his/her integrity is checked by the authentication system before giving the access to actual data. Let's consider the person intercept between the actual user and the system and tries to hack the data.

2. Man-in-the-Middle Attack.

In this module, an attacker may intercept during the authentication of a service provider with the certificate authority, and upload unwanted files into Data owner's Account or Download the important files uploaded by the Data owner.

V. Tools Used For Implementing Cloud

In the proposed model we are using the following tools:

A. Open Stack Cloud

The Open Stack Cloud platform is open source software for building private and public clouds. Predominantly acting as an infrastructure as a service. Platform, it is free and open-source software released under the terms of the Apache License.

B. Word Press

Word Press is a free and open source blogging tool and a content management system (CMS) based on PHP and MySQL, which runs on a web hosting service. Features include a plug-in architecture and a template system. Word Press is the most popular blogging system in use on the Web.

VI. Experiment And Result

We tested our CIA framework by setting up a small cloud, using the Open Stack Platform; the test environment consists of several Open SSL-enabled servers. Each of the servers is installed with Open Stack. Open Stack is an open source cloud implementation for Linux-based systems. We set to work Linux-based servers running Ubuntu 12.04 OS. Each server has a 64-bit Intel Quad Core processor, 4 GB RAM, and a 500 GB Hard Drive.

A. Experimental Results:

In the experiments, we first examine the time taken to create log file and then measure the overhead in the system. With respect to time, the overhead can occur at three points: at the time of the authentication, during uploading of files record, and at the time of downloading of the logs. Also, with respect to storage overhead, we notice that our architectures very lightweight, in that the only data to be stored are provided by the actual files and the associated logs. In particular, as proposed, multiple files can be managed by the same logger component. To this extent, we checked whether a single logger component, used to manage more than one file, results in storage overhead.

B. Log Creation:

In this we are concerned in finding out the time taken to create a log file when there are entities continuously accessing the data, causing continuous logging. With this experiment one can figure out the amount of time to taken will be minimum, keeping things like space constraint or network traffic in mind.

C. Authentication Time:

The authentication time will be completely based on the network traffic and if provided more servers it will not be a matter of concern. Though the user must make use of the USB device which was used during the registration process for the authentication.

VII. Conclusion And Future Work:

We introduced modern approaches for secured logging in and providing safe access to the data in the cloud with an auditing mechanism. Our approach allows the data owner to not only audit his content but also make sure of proper authentication and authorization by avoiding attacks such as MIM. In future, we plan to filter our approach to even more heights and tackle other attacks. And we would like to enhance our architecture from user end which will allow the users to check data remotely in an efficient manner in multi cloud environment.

References:

[1] Ensuring Distributed Accountability for Data Sharing in the Cloud Author, Smitha Sundareswaran, Anna C.Squicciarini, Member, IEEE, and Dan Lin, IEEE Transactions on Dependable and Secure Computing ,VOL 9,NO,4 July/August 2012

[2] Amlan Jyoti Choudhury, Pardeep Kumar,Mangal Sain1 "A Strong User Authentication Framework for Cloud Computing '1 Conf. Cloud Computing, 2011.

[3] Pankaj Kumar Singh,Ajit kumar, R.Karthikeyan "Ensuring Distributed Accountability for Data Sharing in the Cloud", Volume 3, Issue 3, March 2013

[4] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li,"Enabling public auditability and data dynamics for storages security in cloud computing", in INFOCOM.IEEE,2010.

[5] Epuru Madhavarao, M Parimala, Chikkala JayaRaju, " Data sharing in the cloud using Distributed Accountability.", *Volume 2, Issue 6, June 2013*

[6] Ryan K L KO, Peter Jagadpramana, Miranda Mowbray, Siani Perason, Markus Kirchberg, Qianhui Liang, Bu Sung Lee. Trust Cloud: A Framework for Accountability and Trust in Cloud Computing", June 22, 2011.