INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

Design And Development Of Novel Distributed Information Monitoring Framework To Check Actual Information Usage Over Cloud

Amandeep Kaur
Student, CSE Department, Gurukul Vidhapeeth, Banur, Patiala, Punjab, India
Satinderpal Singh
Professor, CE Department, GVIET, Banur. India

Abstract :
Cloud computing is the use of computing of sources (hardware and software) that are delivered as a service over a network (typically the internet). Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Here the security breaches are raised. Users fear losing control about their data (like personal, professional, financial, Health), so that they needed to account their data, which are stored in the cloud. To address this problem, This paper presents a framework CIA for accountability and auditing which is used to protect user's data and also monitor the actual usage of data in the cloud. In particular, a logging mechanism is provided for the user's data with access policies, and ensures that any access to their data will trigger authentication, by this mechanism data owner may know his/her data is handled as per his access policies.. In this paper we use the cloud information accountability (CIA) framework for the data sharing in which use algorithm for giving authority to access data by the CIA framework for resolving privacy and security risks within the cloud. By means of the CIA, data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed. The distributed auditing mechanism is followed and information about the user is collected simultaneously in-order to monitor the usage of data.

Key words:*Cloud computing, accountability, auditing, CIA framework*

1.Introduction

The Cloud Information Accountability framework proposed in this work conducts automated logging and distributed auditing of relevant access performed by any entity, taken out at any point of time at any cloud service provider. It has two major components: logger and log harmonizer. In the Proposed System, a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centred approach that enables enclosing our logging mechanism together with users' data and policies . Accountability is the most critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. Accountability is the agreement to act as in authority proctor of the personal information of others, to take accountability for security

2.Existing System

Cloud provides the space for users to store data and use the services that are available in the cloud.
It records the error correction information sent by the JARs, which allows it to auditor the loss of any logs from any of the JARs. In addition, this approach can handle personal identifiable information provided they are stored as image files (they contain an image of any textual content, for example, the SSN stored as a .JPG file). To allay users' concerns, it is necessary to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users required 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. Conventional access control approaches made for closed domains such as databases and operating systems, or approaches with a centralized server in distributed environments, While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data.

3.Problems

Firstly,The data processed on clouds is often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. This may lead to deficit of data and packets may be delayed and corrupted and also the Data Management and the Services are not Trust Worthy. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, information handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

3.1.Disadvantages

Although the Cloud computing is vast developing technology, the database management system does not have a trustworthiness.

4.Related Work

In this section, we first review related works addressing the privacy and security issues in the cloud. Then, we concisely discuss works which adopt similar techniques as our approach but serve for different purposes.

4.1.Cloud Privacy And Security

Cloud computing has raised a range of important privacy and security issues [9], [10] .Such issues are due to the fact that, in the cloud, users' data and applications reside at least for a certain amount of time on the cloud cluster which is owned and maintained by a third party. Concerns emerge since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. Researchers have inquired accountability mostly as a provable property through cryptographic mechanisms, particularly in the context of electronic commerce .

5.Overview Of Our Proposed Work

To overcome the above problems, we propose a novel method, namely Cloud Information Accountability (CIA) framework, based on the notion of information accountability. In which Data Owner can upload the data or user can download the data into the cloud server after put request to the CIA. User can subscribe into the cloud server with certain access policies such as read, write and copy of the original data. The Loggers and Log Harmonizer will have a track of the access logs and reports to the data owner. This Process ensures security. In CIA (Cloud information accountability) framework we propose solutions by accountability and auditing in cloud .

- **User identity:** To reduce the overhead in proving access control based on user, we will use Attribute based access control. Based on user attributes, access policy will be defined. User matching to this attributes will be given access to data items. This way user management will become easier and also user revocation is easy.
- **Fine grained access of data items**: For each data item, attributes for accessing the data is defined and the user matching to their attributes policy will get only the portion he/she entitled to.

The software architecture of accountability and auditing is sketched below as in fig 1.

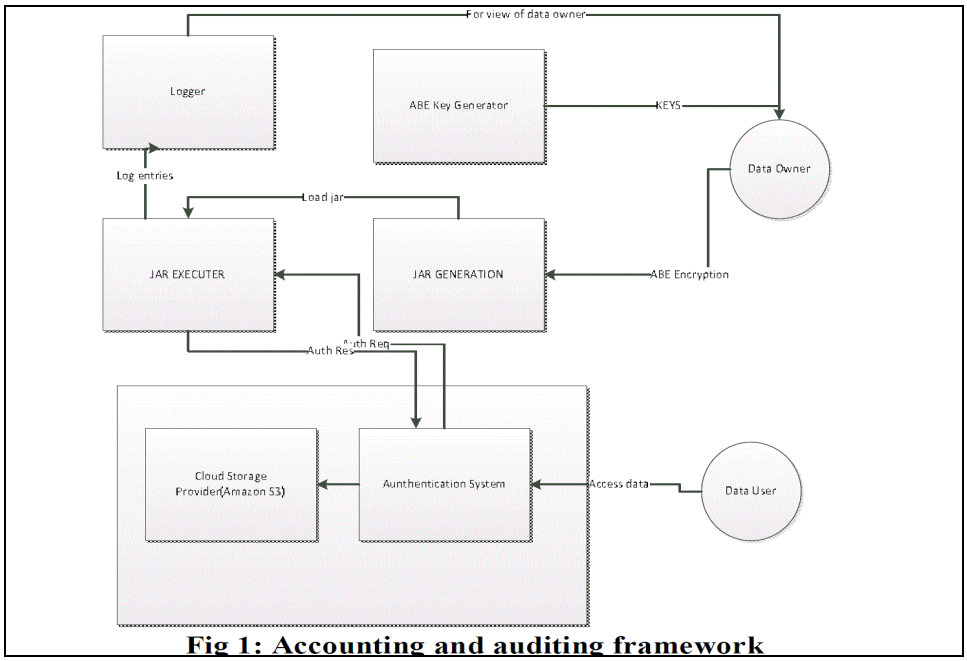


Fig 1: Accounting and auditing framework

Figure 1

In our Framework for accountability and accounting first the data owner will set the policies for the data which data owner wants to place in the cloud using CIA and send it to the cloud service provider (CSP) enclosed in JAR files (here we have considered Amazon cloud storage). Any access to the data by data user will be automatically checked for its authentication and logs record for each data item will be created by logger and sent to data owner for monitoring the data usage. The major components of Accountability and Accounting framework are briefly explained below:

- **Logger:** The logger is strongly bundled with user's data and policies (when user upload the data, the access policies are written). Its main tasks include automatically logging access to data item, it also control the data access even after it is downloaded by some user.
- **Jar module:** It generates a single jar for each data item, when the data item is uploaded. This release the overhead of generating multiple inner jar this may take more time .

6.Implementation

Modules

- User/Data Owner
- Cloud Sever
- Certificate Authority
- Logger
- Access Privileges
- Push And Pull
- Random Set Generation And Verification

6.1.User/Data Owner

User is the person is going to see or download the data from the Cloud server. To access the data from the Cloud server, the users have to be registered with the cloud server. So that the user has to register their details like username, password and a set of random numbers. This is the information that will stored in the database for the future authentication. Data Owner is the Person who is going to upload the data in the Cloud Server. In order to upload the data into the Cloud server, the Data Owner has to be registered in the Cloud Server. Once the Data Owner registered in cloud server, the space will be assigned to the Data Owner.

6.2.Cloud Server

Cloud Server is the area where the user going to request the data and also the data owner will upload their data. Once the user send the request regarding the data they want, the request will ne first send to the Cloud Server and the Cloud Server will forward your request to the data owner. The data Owner will send the data the data the user via the Cloud Server. The Cloud Server will also manage the Data owner and Users' information in their Database for future purpose.

6.3.Logger

The Logger is maintained by the Cloud Server. Loggers have the details of the data owner and users who are accessing the Cloud Server. So the Logger will be more useful for many purposes. Like which user / data owner accessing the Cloud Server, accessed at the particular time and the IP address from which the data is requested by user etc.

6.4.Certificate Authority

The Certificate Authority is used to verify the Cloud Server is recognized or not. The Cloud Server has to be recognized by the certificate authority. If not recognized, the Cloud Server is a Fraudulent Server. The data owner can check the whether the recognized or not. Because the data owner is going to upload their data in the Cloud Server

6.5.Access Privileges

The access privileges are set by the data owner for accessing their data. Some Owners will provide read only, some of them will allow read and download. The Cloud Server will send the dynamic intimation when the user is accessing the data beyond their limits. This increases more security while sharing the data in the Cloud.

6.6.Push And Pull Concept

- Push: For the every periodical time the Cloud Server will send the access details of the user to the

data owner. So that the Data Owner may able to know who're all the accessing their data at the particular time period. During the registration phase, the Data owner will ask by the Cloud Server whether they're choosing the push or pull method 4.2.6.2. **Pull**: In the Pull method, the data owner has to send the request to the Cloud Server regarding the access details of their data up to the particular time. Then the Cloud Server will send the response to the Data Owner regarding the user's access details.

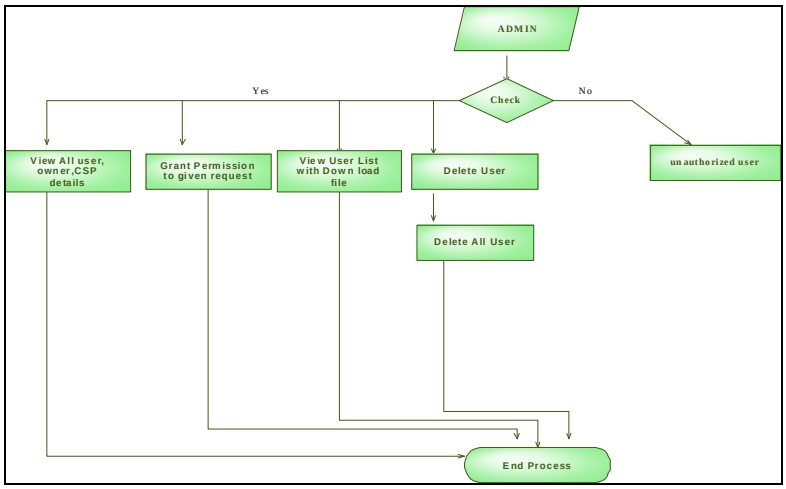


Figure 2: Admin Login

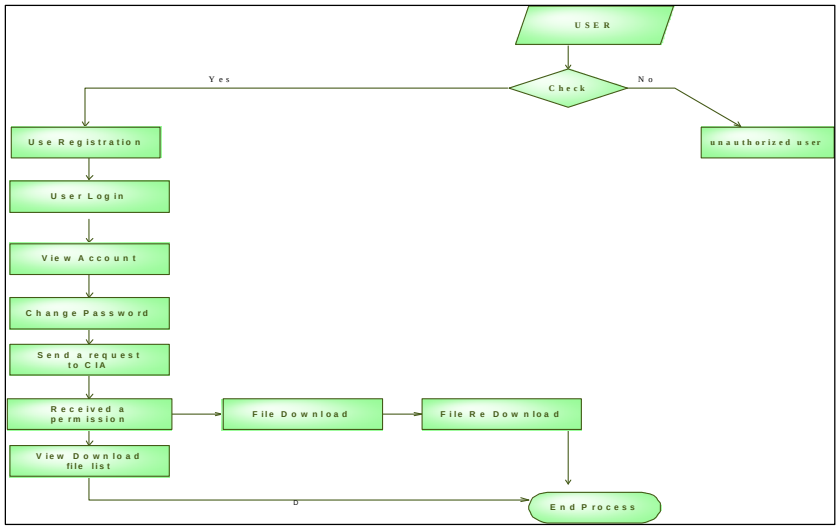


Figure 3: User Login

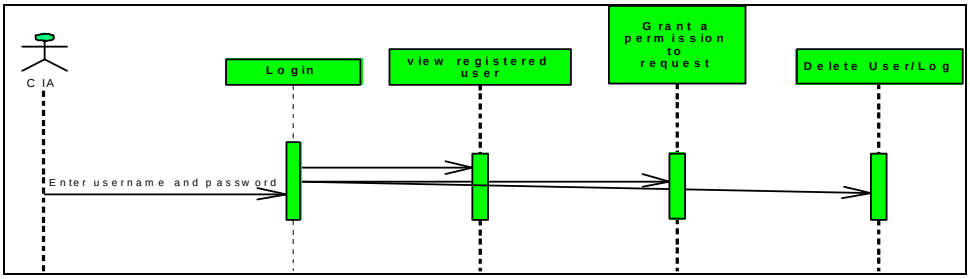


Figure 4: CIA

7.Algorithm Evolution

The algorithm here used is Log Retrieval Algorithm for push and pull modes. The algorithm presents logging and synchronization steps with the harmonizer in case of Pure Log.. If no response is received, the log file records an error. The data owner is then alerted via emails, if the JAR is configured to send error notifications. Once the handshake is done, the interaction with the harmonizer proceeds, using a TCP/IP protocol.Our auditing mechanism has two fundamental advantages. First, it guarantees a high level of availability of the logs. Second, the usage of the harmonizer minimizes the amount of workload for human users in going through log files sent by different copies of JAR files.

Algorithm:

get UID
get PWD
if database entry = UID $ PWD at CIA level
Acess to user type

If type=”user”
View members

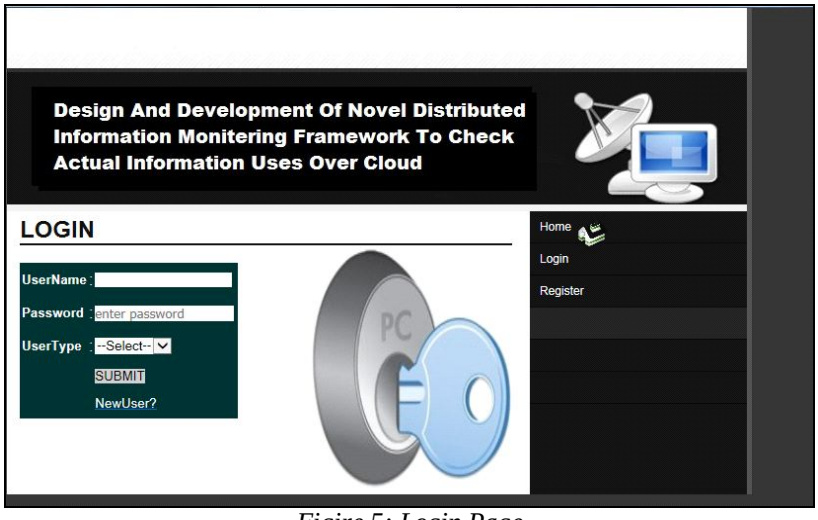
Request= File downloading or redownloading to CIA
If Authenticate
Download done
Else
Not
End
End
Else if type=”owner’
View member

Request= File upload, Assign rules
If authenticate And request accepted
File upload
Else
Not
End
End

Else if type=”CIA”
Acess of all data uploaded
Detail of members

Rest detail of monitoring framework is in database
End
End

8.Results



Figire 5: Login Page

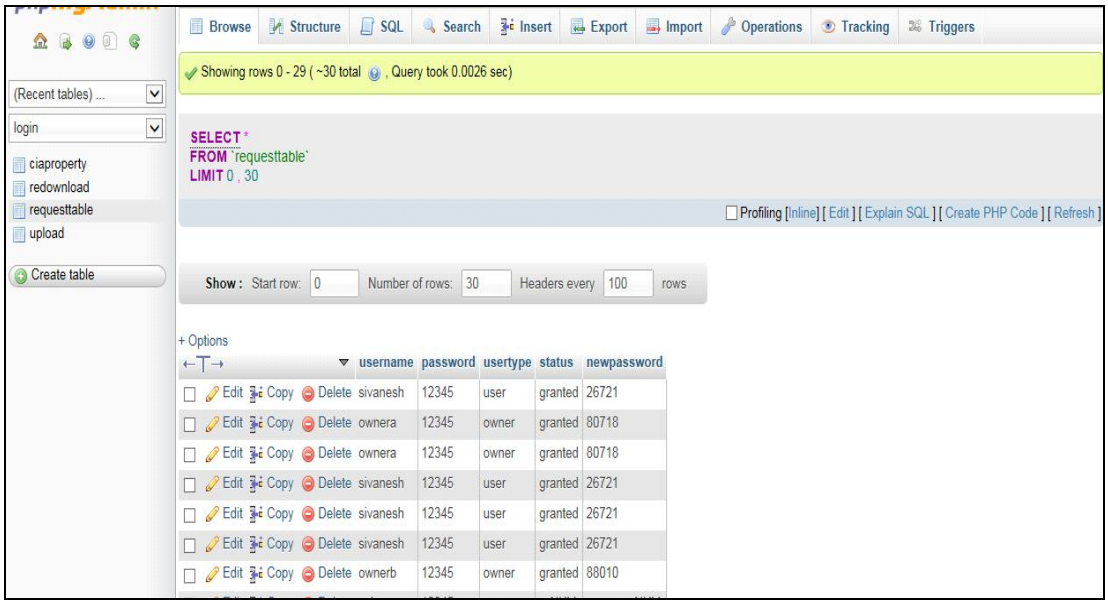


Figure 6: Requestable Data

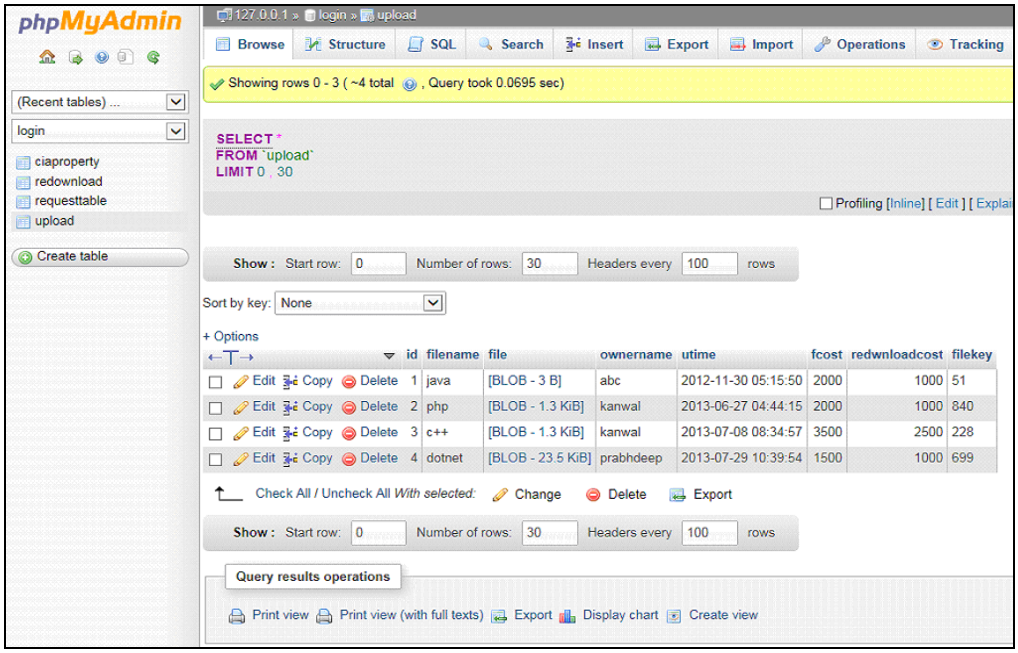


Figure 7: Upload Page By Owner

9.Conclusion

We proposed innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism. Our approach allows the data owner to not only audit his content but also enforce strong back-end protection if needed. Moreover, one of the main features of our work is that it enables the data owner to audit even those copies of its data that were made without his knowledge. This paper presents effective mechanism, which performs authentication of users by CIA and create log records of each data access by the user. Data owner can audit his content on cloud, and he can get the confirmation that his data is safe on the cloud. Data owner should not worry about his data on cloud using this mechanism and data usage is transparent, using this mechanism

In the future, we plan to refine our approach to verify the integrity of the JRE and the authentication of JARs. In future we would like to develop a cloud, on which we will install JRE and JVM, to do the authentication of JAR. Try to improve the security of stored data and to reduce the log record generation time For example, we will investigate whether it is possible to leverage the notion of a secure

JVM being developed by IBM. This research is aimed at providing software tamper resistance to Java applications. In the long term, we plan to design a comprehensive and more generic object-oriented approach to facilitate autonomous protection of travelling content. We would like to support a variety of security policies, like indexing policies for text files, usage control for executables, and generic accountability and provenance controls. In the future, we plan to develop an application to protect the shared data in the cloud with more security using encryption.

10.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) Hsio Ying Lin,Tzeng.W.G, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding ",IEEE transactions on parallel and distributed systems,2012.
3) S. Pearson , Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf. Cloud Computing (cloudcom),,2009
4) S Sundareswaran, A. Squicciarini, D. Lin, and S. Huang, "Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.
5) Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, 2012.
6) D.J. Weitzner, H. Abelson, T and G.J. Sussman, "Information Accountability," Comm. ACM. .
7) Hightower J, Borriello G. "Location Systems for Ubiquitous Computing." Computer 2001;.
8) Hsio Ying Lin,Tzeng.W.G, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding ",IEEE transactions on parallel and distributed systems,2012.
9) Yan Zhu, Hongxin Hu, Gail Joon Ahn, Mengyang Yu, "Coopera-tive Provable Data Possession for Integrity Verification in Multi-Cloud Storage" , IEEE transactions on parallel and distributed systems,2012
10) Muthulakshmi V, Ahamed Yaseen A, , " Enabling Data Security for Collective Records in the Cloud ", International Journal of Recent Technology and Engineering (IJRTE) , Volume-2, Issue-1, March 2013
11) Pankaj Kumar Singh , Ajit kumar, R.Karthikeyan "Ensuring Distributed Accountability for Data Sharing in the Cloud" ,IJARCSSE volume3 ,issue 3,march 2013
12) P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, Aug. 19,2012