ISSN 2395-1621

Cloud Information Accountability (CIA) framework based on Information Accountability

[#1]Mr. Borse Sagar Ravindra, [#2]Mr. Dengale Pritam Vijay
[#3]Mr. Dorge Yogesh Walmik, [#4]Miss.Jagtap Priyanka Raosaheb

[1]sagarborse870@gmail.com
[2]prit0505@gmail.com
[3]yogeshdorge0909@gmail.com
[4]priyanka.r.jagtap@gmail.com

[#1234]Dept. of Computer Engineering H.S.B.P.V.T. COE, Kashti
Tal:-Shrigonda, Dist-Ahmednagar
Maharashtra, India

ABSTRACT

Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To solve the above problem in this paper we provide effective mechanism to using accountability frame work to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. Accountability is checking of authorization policies and it is important for transparent data access. We provide automatic logging mechanisms using JAR programming which improves security and privacy of data in cloud. To strengthen user's control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches

Keywords: **Cloud computing, data sharing, information accountability framework, Provable data possession, Logging, auditability, accountability, data sharing**

ARTICLE INFO

Article History

Received :7th October 2015

Received in revised form :

7th October 2015

Accepted : 13th October , 2015

Published online :

16th October 2015

I. INTRODUCTION

Cloud computing is a technology which uses internet and remote servers to store data and application. In cloud there is no need to install particular hardware, software on user machine, so user can get the required infrastructure on his machine in cheap charges/rates. Cloud services where services made available to users on demand via the internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. Now Days, there are a number of noticeable commercial and individual cloud computing services like Amazon, Google, Microsoft, Yahoo, and Sales force [19]. Examples of cloud services include online backup solutions and data storage, Web-based e-mail services, hosted office suites and document collaboration services, database processing more. Cloud computing is an infrastructure which provides useful, on demand network services to use various resources with less effort. Features of Cloud computing are, huge access of data, application, resources and hardware without installation of any software, user can access the data from any machine or anywhere in the world, business can get resource in one place, that's means cloud computing provides scalability in on demand services to the business users. Everyone kept their data in cloud, as everyone kept their data in cloud so it becomes public so security issue increases towards private data. Furthermore, users may not know which machines actually process and host their data. While enjoying the advantage brought by this new technology, users also start concerned about losing control of their own data. The data processed on

clouds are often deployed, causes to a number of issues related to accountability like the handling of personally identifiable information for cloud user.It is more important for cloud users that monitor their usage of their data in the cloud. For example, users have 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. First one is the, data handling can be outsourced/deployed by the direct cloud service provider (CSP) to other user in the cloud and these users can also instruct the tasks to others, and so on. Second, users are allowed to join and leave the cloud in a flexible manner. Because of this characteristic, data handling in the cloud goes through a complex and dynamic service chain which does not exist in traditional environments. To overcome the above problems, new novel approach, namely Cloud Information Accountability (CIA) framework, based on the concept of information accountability. Information accountability focuses on keeping the data usage transparent and tractable. IA framework provides end-to end accountability in a highly distributed fashion. Most important feature of the CIA is that its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. In CIA, data owners can track not only whether or not the service-level agreements are being honored, but also enforce access and usage control rules as needed. Associated with the accountability feature, also develop two distinct modes for auditing: push mode and pull mode. The push mode mentions to logs being periodically sent to the data owner or stakeholder while the pull mode mentions to an alternative approach whereby the user (or another authorized party) can retrieve the logs as needed. In this existing approach toward addressing these issues is to hold and extend the programmable capability of JAR (Java Archives) files to automatically log the usage of the users' data by any entity in the cloud. Users will send their data along with any policies according to their choice such as access control policies and logging policies that they want to enforce, enclosed in JAR files, to cloud service providers. Any access to the data will trigger an automated and authenticated logging mechanism local to the Jars. Decentralized logging mechanism meets the dynamic nature of the cloud but also imposes challenges on ensuring the integrity of the logging. To cope with this issue, we provide the JARs with a central point of contact which forms a link between them and the user. It records the error correction information sent by the JARs, which allows it to monitor the loss of any logs from any of the Jars. Currently, we focus on image files since images represent a very common content type for end users and organizations (as is proven by the popularity of Flickr [14]) and are increasingly hosted in the cloud as part of the storage services offered by the utility computing paradigm featured by cloud computing. Further, images often reveal social and personal habits of users, or are used for archiving important files from organizations. In addition, our 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).

Cloud provides three service models, which are; platform as a service, infrastructure as a service and software as a service. Under the Database as a service, this is having four parts which are as per mentioned below,

- Encryption and Decryption - For security purpose of data stored in cloud, encryption seems to be perfect security solution.
- Key Management - If encryption is necessary to store data in the cloud, encryption keys can't be store their, so user requires key management.
- Authentication - For accessing stored data in cloud by authorized users.
- Authorization – Rights given to user as well as cloud provider.

II. RELATED WORK

In this, we study on related works, which addresses the privacy and security issues in the cloud. Then, we briefly discuss works which adopt similar techniques as our approach but serve for different purposes.

A. 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.

B. Other Related Techniques

With respect to Java-based techniques for security, our methods are related to self-defending objects (SDO) [17]. Self-defending objects are an extension of the object-oriented programming paradigm, where software objects that offer sensitive functions or hold sensitive data are responsible for protecting those functions/data. Similarly, we also extend the concepts of object-oriented programming. The key difference in our implementations is that the authors still rely on a centralized database to maintain the access records, while the items being protected are held as separate files. In previous work, we provided a Java-based approach to prevent privacy leakage from indexing [39], which could be integrated with the CIA framework proposed in this work since they build on related architectures.

In terms of authentication techniques, Appeal and Felton [13] proposed the Proof-Carrying authentication (PCA) framework. The PCA includes a high order logic language that allows quantification over predicates, and focuses on access control for web services. While related to ours to the extent that it helps maintaining safe, high-performance, mobile code, the PCA's goal is highly different from our research, as it focuses on validating code, rather than monitoring content. Another work is by Mont et al. who

proposed an approach for strongly coupling content with access control, using Identity-Based Encryption (IBE) [26].

In previous techniques it ensures that no one can add or remove entries in the middle of a provenance chain without detection, so that data are correctly delivered to the receiver. Differently, our work is to provide data accountability, to monitor the usage of the data and ensure that any access to the data is tracked.

II. CLOUD INFORMATION ACCOUNTABILITY

To solve the security issues in cloud; other user can't read the respective users data without having access. 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 track usage of data in the cloud. Accountability is necessary for monitoring data usage, in this all actions of users like sending of file are linked to the server, that performs them and server maintain secured record of all the actions of past and server can use the past records to know the correctness of action. It also provides reliable information about usage of data and it observes all the records, so it helps in make trust, relationship and reputation. So accountability is for verification of authentication and authorization. It is powerful tool to check the authorization policies [9].Accountability describes authorization requirement for data usage policies. Accountability mechanisms, which rely on after the fact verification, are an attractive means to enforce authorization policies [7].

There are 7 phases of accountability

1. Policy setting with data
2. Use of data by users
3. Logging
4. Merge logs
5. Error correctness in log
6. Auditing
7. Rectify and improvement.

These phases may change as per framework First the data owner will set the policies with data and send it to cloud service provider (CSP), data will be used by users and logs of each record will be created, then log will be merged and error correction in log has been done and in auditing logs are checked and in last phase improvement has been done [12].

the Fig 1 Steps of accountability is given these are 7 steps each step is important to perform next step, accountability is nothing but validation of user actions means user having rights for accessing this data or not. Suppose user will do misuse of data or resources then network or data owner will take action on it so users, businesses and government should not bother about their data on cloud.

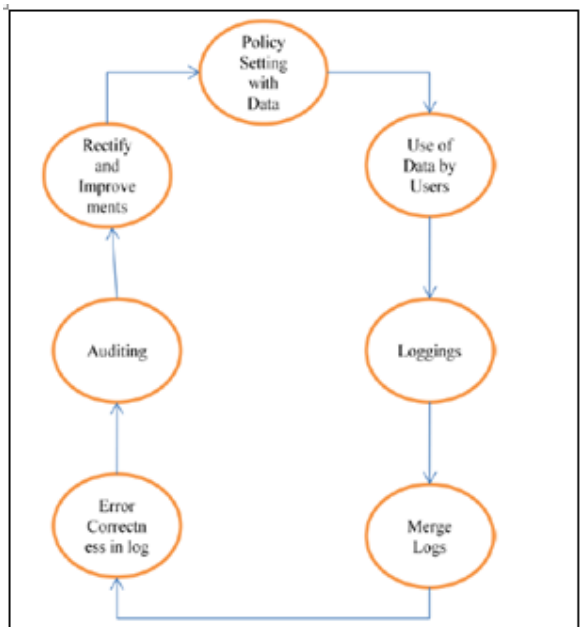


Fig 1:Phases of Accountability

IV. AUTOMATED LOGGING MECHANISM

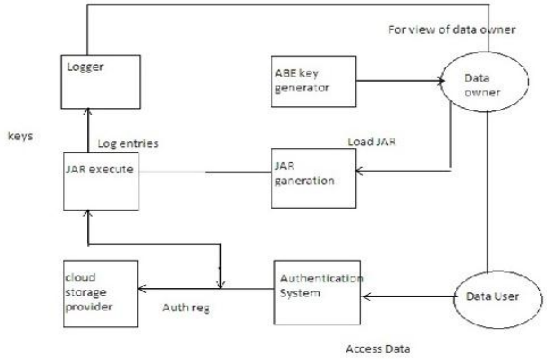
In this section, we first elaborate on the automated logging mechanism and then present techniques to guarantee dependability.

V. SECURITY DISCUSSION

We now analyze possible attacks to our framework. We assume that attackers may have sufficient Java programming skills to disassemble a JAR file and prior knowledge of orca architecture. We first assume that the JVM is not corrupted, followed by a discussion on how to ensure that this assumption holds true.

A. Attacks on JAR files:

The common attack that we can assume is accessing the detain JAR file without being noticed. This kind of attacks can be found out by auditing. In this, if someone tries to download the JAR files, the actions are recorded by the logger and the log record is sent to the user. By this steps data owner will be have knowledge of his/her JAR file download.



B. Unauthorized user:

If some unauthorized user who don't have permission *to access that data*, in this first we have to check the his/her integrity by the authentication system before giving the access to actual data. Let us consider third party tries to access the data or hack the data. But he will receive the disassembled Jar file and log record which is encrypted and if he/she need to decrypt it to get the actual data, and also breaking the encryption is computationally complex.

VI. PERFORMANCE STUDY

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

Implementation:

Here we have developed our framework in java platform and for cloud storage we have used Amazon web service s3. We tested the framework by uploading and downloading image files, as image files are common content type for users and organizations nowadays (for example Flickr). The framework is light because the data's are stored in cloud and to do that time taken is less. Next, the JAR module acts as compressor by compressing the files which reduces the memory space.

VII.THE LOGGER STRUCTURE

We leverage the programmable capability of JARs to conduct automated logging. A logger component is a nested Java JAR file which stores a user's data items and corresponding log files. The main responsibility of the outer JAR is to handle authentication of entities which want to access the data stored in the JAR file. In our context, the data owners may not know the exact CSPs that are going to handle the data. Hence, authentication is specified according to the servers' functionality (which we assume to be known through a lookup service), rather than the server's URL or identity. For example, a policy may state that Server X is allowed to download the data if it is a storage server. As discussed below, the outer JAR may also have the access control functionality to enforce the data owner's requirements, specified as Java policies, on the usage of the data. A Java policy specifies which permissions are available for a particular piece of code in a Java application environment. The permissions expressed in the Java policy are in terms of File System Permissions. However, the data owner can specify the permissions in user-centric terms as opposed to the usual code-centric security offered by Java, using Java Authentication and Authorization Services. Moreover, the outer JAR is also in charge of selecting the correct inner JAR according to the identity of the entity who requests the data.

VII. SHA ALGORITM AS CRYPTOGRAPHIC ADVANCEMENT

SHA-1 is the most widely used of the existing SHA hash function designed by the National Security Agency (NSA) and is employed in several widely-used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives.

Mathematical Model:

The log records(Lr) are generated as –

- Lr = r1,r2,r3,r4....rk
  rk = (id,action,T,loc,h((idaction,T,loc)ri-1...r1),sig)
- rk = log record
- id = user identification
- action = perform on user's data
- T = Time at location loc
- loc = Location
  h((id,action,T,loc)ri-1...r1) = checksum component
- sig = signature of records by server
- Checksum is computed using hash function
  H[i] = f(H[i-1],m[i])

IX. CONCLUSION

It is more important today, to secure unwanted and unauthorized disclosure of their confidential data from the third party. In this paper, the authors have studied and review the security and privacy issues in cloud computing. This paper presents effective mechanism, which performs authentication of users and create log records of each data access by the user. Data owner has ability to audit his content on cloud, and he can get the confirmation that his data is safe on the cloud. Data owner also able to know the duplication of data made without his knowledge. Data owner has secure storage his data on cloud using this mechanism and data usage is transparent, using this mechanism.

ACKNOWLEDGMENT

The authors would like to thanks the Department of Computer Engineering H.S.B.P.V.T. College of Engineering & Research, Ahemadnagar, India for the guidance and cooperation.

REFERENCES

[1] B.Crispo and G.Ruffo, "Reasoning about Accountability within".

[2]Delegation" Proc. Third Int"l Conf. Information and Comm. Security(ICICS), pp. 251-260, 2001.

[3] S. Pearson, Y. Shen, and M. Mowbray," A privacy Manager

[4]Cloud Computing," Proc. Int'l Conf. Cloud Computing cloudcom), pp.90-106, 2009.

[5] S. Pearson and A. Charlesworth, "Accountability as a Way Forwardfor Privacy Protection in the Cloud, "*Proc First Int'l conf. Cloud*Computing, 2009.

[6]R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "ALogic for Auditing Accountability in Decentralized Systems," Proc. IFIPTC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201,2005.

[7]A. Squicciarini , S. Sundareswaran and D. Lin, " PreventingInformation Leakage from Indexing in the Cloud," *Proc. IEEE Int'l* Conf.Cloud Computing, 2010

[8]Q. Wang, C. Wang, K. Ren, W. Lou and J. Li,"Enabling publicauditability and data dynamics for storages security incloud computing", inINFOCOM.IEEE,2010,pp. 525-533
.

[9]C.Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving publicauditing for data storage security in cloud computing,"in INFOCOM. IEEE,2010, pp. 525–533.

[10]D. Boneh and M.K. Franklin, "Identity-Based Encryption from theWeil Pairing," Proc. Int‟l Cryptology Conf.

