ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Distributed Accountability and Auditing Mechanism in Cloud

Swapnil Neharkar [1], B.M. Patil [2]

Department of Computer Science Engineering, MBE'S COE, Ambajogai, Maharashtra, India[1]

Department of Computer Science Engineering, MBE'S COE, Ambajogai, Maharashtra, India[2]

ABSTRACT: The widespread use of Cloud computing has opened up new challenges by introducing different types of trust scenario. The lack of confidence in trusting information flow in cloud has become common. Users data are usually processes remotely in unknown machine that do not owned or operated by user. As user fears of losing control of their own data like Finical, Health, Personal etc. In addition to this, through some privacy protection controls technique only concrete on preventive control. This paper presents a frame work for distributed accountability and auditing which is used to protect user's data and also monitor the actual usages of data in cloud. In particular logging mechanism is provided for the user data is handled as per his access policies. Distributed auditing mechanism is followed and information of user is collected simultaneously in order to monitor the user data. We have use the PDF, .Doc and Jpg file and take the results.

KEYWORDS: Cloud Computing, Information Accountability Framework, Privacy, Auditing, Security.

I. INTRODUCTION

Cloud computing is an emerging paradigm in the computer industry that puts entire computing infrastructure hardware and software, applications etc. online. It uses internet and remote, central servers to maintain data and applications. The cloud computing core concept is simply, a geographical shift in the location of our data from personal computers to a centralized server or cloud. Cloud Computing is a step towards the evolution of on demand information technology services and products .Cloud computing is a means by which highly scalable and fully technology based services can be easily consumed over the internet on an as-needed basis. Although there are many benefits to adopt Cloud Computing but still there are some significant barriers to adoption. The convenience and efficiency of this technology comes with security risks and data privacy. Significant barrier to the adoption of cloud services is the user's fear of losing confidential data and privacy in the cloud. Privacy is an important and basic human right that encompasses the right to be left alone, to provide this right many techniques are proposed under different systems and security models. There are possibilities that data can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and these entities can also allocate the task of data management to others, and so on. Being flexible in nature entities are all old to join and leave cloud on their wish. This cause's data handling takes place through a complex and dynamic hierarchical service chain which does not exist in conventional environments. To overcome the above stated problems, a new approach called Cloud Information Accountability (CIA) framework

II. LITERATURE SURVEY

In this section review related works addressing security in cloud. Security issue is very important in cloud there are many techniques available so here is review of all these.

Security and Privacy issues in cloud

Provide a language which allows providing data with policies by agent; here agent has to prove their action and authorization to use particular data. In this technique data owner attach Policies with data that contain a description of which actions are all old with which data, but there is the problem of Continuous auditing of agent. But there work has

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

also provided solution that monitors incorrect behaviour of agent and agent has to give justification for their action, after that authority will check the justification [1]. A privacy manager mechanism was given by S. Pearson in which the user's data is in encrypted form in cloud and evaluation is done on encrypted data. The privacy manager makes readable data from result of evaluation manager to get the correct result. As in obfuscation data is not present on Service provider's machine so there is no risk with data and hence data is safe on cloud. But this solution is not suitable when input data is large where this method can still require a large amount of memory. presents mechanism in which policies are decided by the parties that use, store or share the data irrespective of the jurisdiction in which information is processed. But data processed on service provider is in unencrypted at the time of processing so there is a risk of data leakage which becomes disadvantage of this mechanism [2]. There is a method of dynamic auditing protocol proposed by authors in which supports the dynamic operations of the data on the cloud servers, but this method may leak the data content to the auditor as it requires the server to send the linear combinations of data blocks to the auditor. The authors extended their dynamic auditing scheme to be privacy preserving and support the batch auditing for multiple owners. However, due to the large number of data tags, their auditing protocols may incur a heavy storage overhead on the server. Authors have given a three layer architecture which protects information leakage from cloud; it provides three layers to protect data. In first layer the service provider is not all old to view confidential data, in second layer service provider should cannot do the indexing of data, in third layer user specify use of his data and indexing in policies. In this way policies always travel with data [2].

Propose a novel automatic and Enforceable logging mechanism in the cloud. To our knowledge, this is the first time a systematic approach to data accountability through the novel usage of JAR files is proposed. Their proposed architecture is platform independent and highly decentralized, in that it does not require any dedicated authentication or storage system in place but here multiple jar files (inner jars), takes lot of time to execute and latency is noticed by data users [3].

Identity based Encryption (IBE)

The authors proposed identity-based encryption scheme (IBE). The scheme has chosen cipher text security in the random oracle model assuming an alternative of the computational Die-Hellman problem. This system is based on bilinear maps between groups. The example of such map is on elliptic curves. They have given precise definitions for secure identity based encryption schemes and given several applications for such systems. Using standard techniques from threshold cryptography the PKG in their scheme master-key is being distributed so that this key is never available in a single location. Unlike common threshold systems, the authors should that robustness for their systems distributed PKG is free [1].

III. CIA SCHEMA

There is need to provide technique which will audit data in cloud. On the basis of accountability, Cloud Information Accountability (CIA) framework is one mechanism which keeps use of data transparent means data owner should get information about usage of his data. This mechanism support accountability in distributed environment.

Push and Pull Mode

Push mode. In this mode, the logs are periodically pushed to the data owner (or auditor) by the harmonizer. The push action will be triggered by either type of the following two events: one is that the time elapses for a certain period according to the temporal timer inserted as part of the (PDF, .Doc, Jpg etc) file; After the logs are sent to the data owner, the log files will be dumped, so as to free the space for future access logs. Along with the log files, the error correcting information for those logs is also dumped. This push mode is the basic mode which can be adopted by both the Pure Log and the Access Log, regardless of whether there is a request from the data owner for the log files. This mode serves two essential functions in the logging architecture: 1) it ensures that the size of the log files does not explode and 2) it enables timely detection and correction of any loss or damage to the log files.

Pull mode. This mode allows auditors to retrieve the logs anytime when they want to check the recent access to their own data. The pull message consists simply of an FTP pull command, which can be issues from the command line. For naive users, a wizard comprising a batch file can be easily built. The request will be sent to the harmonizer, and the user will be informed of the data's locations and obtain an integrated copy of the authentic and sealed log file.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

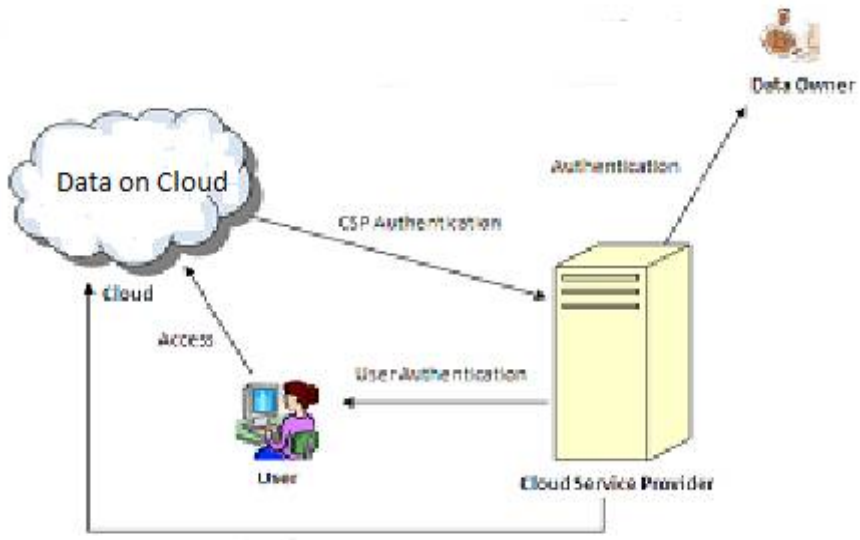

Fig 1: CIA Model with CSP

IV. SECURITY

Man-in-the-Middle Attack

An attacker may intercept messages during the authentication of a service provider with the certificate authority, and reply the messages in order to masquerade as a legitimate service provider. There are two points in time that the attacker can replay the messages. One is after the actual service provider has completely disconnected and ended a session with the certificate authority. The other is when the actual service provider is disconnected but the session is not over, so the attacker may try to renegotiate the connection. The first type of attack will not succeed since the certificate typically has a time stamp which will become obsolete at the time point of reuse. The second type of attack will also fail since renegotiation is banned in the latest version of Open SSL and cryptographic checks have been added.

V. RESULT ANALYSIS

We first bring out setting of the test environment and then present the performance study of our system. In the experiments, We first examine the time taken to create a log file and then measure the overhead in the system. With respect to time, the overhead can occur at three points: during the authentication, during encryption of a log record, and during the merging of the logs. Also, with respect to storage overhead, We notice that our architecture is very light, in that the only data to be stored are given by the actual files and the associated logs. Further, on behalf of JAR file we have take the results using PDF, .Doc and Jpg file. Multiple files can be handled by the same logger component. To this extent, We investigate whether a single logger component, used to handle more than one file, results in storage overhead.

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 1. At the time of authentication, during encryption of a log record, and at the time merging of the logs, Also with respect to storage overhead We notice that our architecture very light, in that the only data to be storage are provided by the actual files and associated logs. We have use the PDF, .Doc and Jpg file for taking results.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

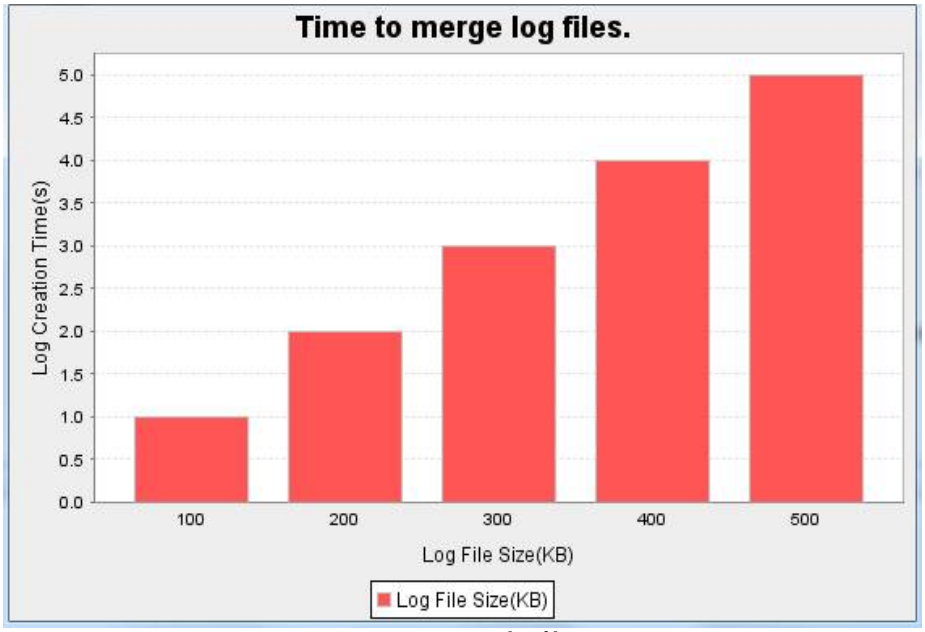

Fig 2: Time to Merge log file

We have taken the amount of time required to merge log file. We confirmed that each of the log files had 0 to 25 percent of record in common with one other. The exact number of records in common was random for each repetition. The time was averaged over 10 repetitions. We tested the time to merge up to 75 log files of (PDF, Jpg, .Doc file) 100kb, 300kb, 500kb each.

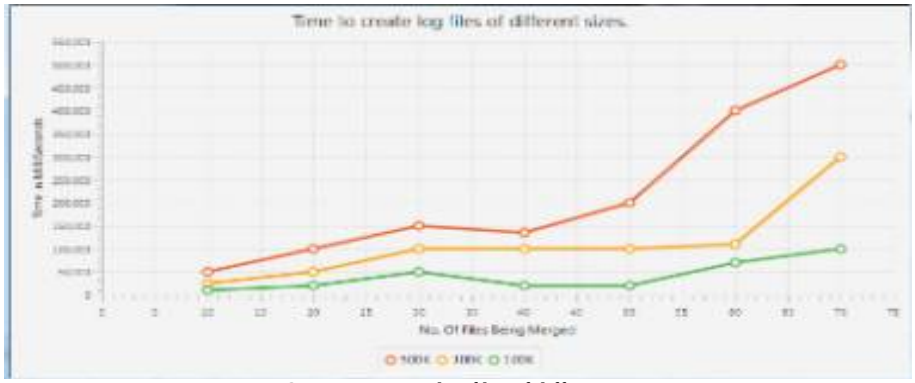

Fig 3: Time to create log files of different sizes

VI. CONCLUSION

We introduced modern approaches for automatically logging any accesses to the data in the cloud together with an auditing mechanism using (PDF, Jpg, .Doc file) for experimental results behalf of JAR file . Our approach allows the data owner to not only audit his content but also enforce strong back end protection. Apart from that We have enclosed PDP methodology to enhance the integrity of owner's data. . In future, and We would like to enhance our architecture from user end which will allow the user's to check data remotely in an efficient manner in multi cloud environment.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

REFERENCES

[1] SmithaSundareswaran, 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, pg 556-568, 2012.
[2] A. Squicciarini , S. Sundareswaran and D. Lin, " Preventing Information Leakage from Indexing in the Cloud," *Proc. IEEE Int'l* Conf.Cloud Computing, 2010
[3] Ensuring Distributed Accountability for Data Sharing in the cloud ,Author Pankal Kumar Singh, Ajit Kumar, R. Karthikeyan from C.S.E. Bharath University, India Vol 3, Issue 3 March 2013 IJARCSSE ISSN: 2277 128X.
[4] Review on Technique to Ensuring Distributed Accountability for Data Sharing in the cloud, Author H.Arun, R.Nilam, R.Namaratha, Vol 2, Issue 10 Oct 2013, ISSN 2278-1021
[5] Just Cloud Website.
[6] T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), first ed. O' Reilly, 2009.
[7] S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang,"Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.