Secure Data Sharing in the Cloud

J. S. Aswathy

M.Tech. Student, Department of Computer and Information Science, Sarabhai Institute of Science and Technology, Trivandrum, India

***Abstract*: Cloud Computing is the use of computing resources that are delivered as a service over internet. Cloud Computing provides various services on demand. Users who want to do business with their data in the cloud is having the fear of losing control of their data. Data Owner who store the data in the cloud should ensure that the data stored in the cloud is secure. To solve this problem accountability is used to keep track of the usage of data. Jar programmable capabilities are used for providing automatic logging mechanism which provide security and privacy of data in the cloud. Security can be further improved by providing software tamper resistance to Java applications.**

***Keywords*: Cloud Computing ,accountability, data sharing ,privacy.**

1. Introduction

Cloud Computing is the use of computing resources that are delivered as a service over the internet. Cloud computing provides on demand services. Cloud provides three service models which include platform as a service(paas), software as a service(saas), infrastructure as a service(Iaas).User may not know the machine which actually process or host their data. While enjoying the convenience brought by this new technology, users start worrying about losing control of their own data [1].

It is very essential to provide security in the cloud. It is very essential to ensure that the data placed in the cloud cannot be accessed by unauthorized users or cannot be modified by hackers. There is a need for the security mechanism which actually keep track of the usage of data in the cloud. Cloud information accountability is used to keep track of the usage of data in the cloud. By means of CIA framework, data owner can track whether or not the service-level agreements are met. It also enforce access and usage control rules. Associated with accountability two distinct modes for auditing is used. They are push mode and pull mode. The push mode refers logs being periodically sent to the data owner. The pull mode refers can be retrieved when needed.

The design of the CIA framework provides challenges including uniquely identifying CSPs, ensuring reliability of the logs etc. Programmable capabilities of the log the usage of the users data by any entity in the cloud. Users will send their data along with any policies 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. In order to ensure the integrity of the logging provide JAR as the central point of contact which record the error correction information by monitoring the loss of any logs from any of the JARS.

Logging and auditing technique helps to ensure that every access to the users data should be correctly and automatically logged. Log files should be reliable and tamper proof to avoid illegal insertion, deletion and modification by malicious parties. Log files should be sent back to the data owner periodically to inform the current usage of data.log files can be retrieved by the data owner when needed regardless of the location where the files are stored.

2. Proposed work

There is a need for adopting a technique for providing auditing of the data in the cloud. Accountability is used for keeping track of the usage of data in the cloud. Accountability helps to ensure whether the data is handled according to the service level agreements. Accountability also ensures that the data kept by the owner is safe on the cloud. Security can further be improved by providing software tamper proof resistance to the java application.

A. Cloud Information accountability framework

The Cloud Information Accountability framework conducts automated logging and distributed auditing of access performed by any entity. It has two major components: logger and log harmonizer.

B. Major Components

The logger is the component which is strongly coupled with the user’s data, so that it is downloaded when the data is being accessed and is copied whenever the datas are copied. Main task include automatically logging access to the data items that it contains, encrypting the log record using the public key of the content owner and periodically sending them to the log harmonizer. Log harmonizer is responsible for auditing. Log harmonizer is responsible for decrypting the logs.

Harmonizer supports two auditing strategies: push and pull. Under the push strategy the log file is pushed back to the data owner periodically. The pull mode is an on-demand approach whereby log file is obtained by the data owner as often as requested. If there exists multiple loggers for the same set of data items the log harmonizer will merge log records before sending to the data owner.

3. Data flow

The overall CIA framework combining data, users, logger and harmonizer is as follows. At the beginning user creates a pair of public and private keys. User then creates logger component which is a JAR file, to store its data items. Then sending the JAR file to the CSP that the user is subscribed to. After succeeding the authentication of the CSP to the JAR the service provider is allowed to access the data enclosed in the JAR. For each time access to the data JAR will automatically generate a log record, encrypt it using the public key distributed by the data owner and store it along with the data. The encryption of log file prevents the unauthorized changes to the file by the attackers. In addition, some log correction information will be sent to the harmonizer to handle the possible log file corruption.

4. Conclusion

An automatically logging and auditing approach is used for the data access in the cloud. This approach allows the data owner not only to audit his content but also enforce strong back end protection if needed. Moreover, one of the main features is that it enables the data owner to audit even those copies of its data that were made without his knowledge**.** An integrity checking is performed to determine whether the data is corrupted or not. Also security is improved by providing software tamper resistance to Java applications.

References

[1] S. Sundareswaran, A. Squicciarini and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," in *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 556-568, July-Aug. 2012.

[2] S. Sundareswaran, A. Squicciarini, D. Lin and S. Huang, "Promoting Distributed Accountability in the Cloud," *2011 IEEE 4th International Conference on Cloud Computing*, Washington, DC, 2011, pp. 113-120.

[3] S. Pearson, Y. Shen, and M. Mowbray, “A Privacy Manager for Cloud Computing,” Proc. Int’l Conf. Cloud Computing (CloudCom), pp. 90-106, 2009.

[4] R. Corin, S. Etalle, J. I. Den Hartog, G. Lenzini, and I. Staicu, “A Logic for Auditing Accountability in Decentralized Systems,” Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[5] R. Jagadeesan, A. Jeffrey, C. Pitcher, and J. Riely, “Towards a Theory of Accountability and Audit,” Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 152-167, 2009.