Middle-East Journal of Scientific Research 20 (6): 758-761, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.20.06.11392

Guarantee Dispersed Responsibility for Data Allocation in the Cloud

K. Sankar, A. Muthukumaravel and S. Kannan

Department of MCA, Bharath University,
Selaiyur, Chennai - 73, Tamil Nadu, 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 address this problem, here, we propose 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-centered approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. 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.

Key words: Enables highly scalable · Cloud services · Emerging technology · Cloud services · Logging mechanism

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 computing is an infrastructure which provides useful, on demand network services to use various resources with less effort [1-8]. 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 any where 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 [9]. Data usage in cloud is very large by users and businesses, so data security in cloud is very important issue to solve. Many users want to do business of his data through cloud, but 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 [1], [8].

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.

Corresponding Author: K. Sankar, Department of MCA, Bharath University, Selaiyur, Chennai - 73, Tamil Nadu, India.

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 [10], in this all actions of users like sending of file are cryptographically 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:

- Policy setting with data
- Use of data by users
- Logging
- Merge logs
- Error correctness in log
- Auditing
- 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 use 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 [11-12].

Modules Description

Cloud Information Accountability (CIA) Framework: CIA framework lies in its ability of maintaining lightweight and powerful accountability that combines aspects of access control, usage control and authentication. By means of the 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.

Distinct Mode for Auditing

Push Mode: The push mode refers to logs being periodically sent to the data owner or stakeholder.

Pull Mode: Pull mode refers to an alternative approach whereby the user (Or another authorized party) can retrieve the logs as needed.

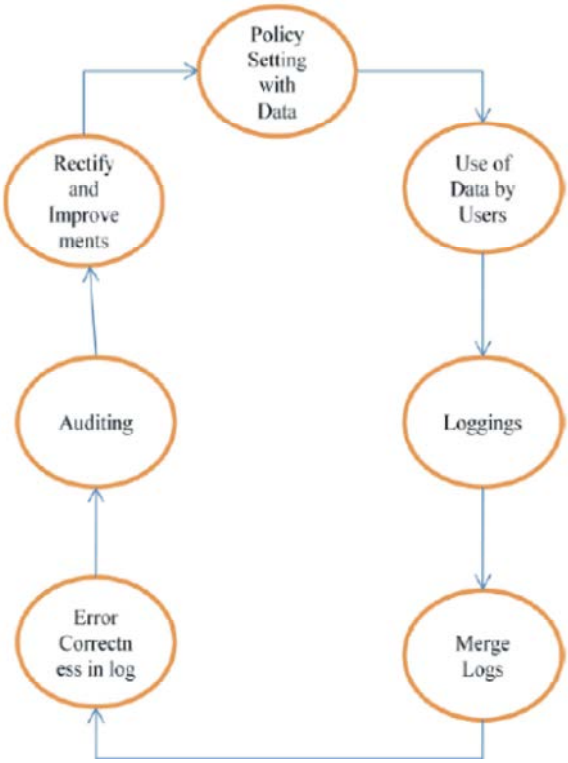
Logging and Auditing Techniques:

- The logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled and require minimal infrastructural support from any server.
- Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify and record the actual operations on the data as well as the time that the data have been accessed.
- Log files should be reliable and tamper proof to avoid illegal insertion, deletion and modification by malicious parties[11]. Recovery mechanisms are also desirable to restore damaged log files caused by technical problems.
- Log files should be sent back to their data owners periodically to inform them of the current usage of their data. More importantly, log files should be retrievable anytime by their data owners when needed regardless the location where the files are stored.
- The proposed technique should not intrusively monitor data recipients' systems, nor it should introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

Major Components of CIA: There are two major components of the CIA, the first being the logger and the second being the log harmonizer. The logger is strongly coupled with user's data (either single or multiple data items). Its main tasks include automatically logging access to 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. It may also be configured to ensure that access and usage control policies associated with the data are honored.

For example, a data owner can specify that user X is only allowed to view but not to modify the data. The logger will control the data access even after it is downloaded by user X. The log harmonizer forms the central component which allows the user access to the log files. The log harmonizer is responsible for auditing.

Phases of Accountability:



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. S. Pearson et al describes privacy manager mechanism in which user's data is safe on cloud, in this technique the user's data is in encrypted form in cloud and evaluating is done on encrypted data, the privacy manager make readable data from result of evaluation manager to get the correct result. In obfuscation data is not present on Service provider's machine so there is no risk with data, so data is safe on cloud, But this solution is not suitable for all cloud application, when input data is large this method can still require a large amount of memory [2]. In [3], the authors present procedural and technical solution both are producing solution to accountability to solving security risk in cloud in this mechanism these policies are decided by the parties that use, store or share that data irrespective of the jurisdiction in which information is processed. But it has limitation that data processed on SP is in unencrypted at the point of processing so there is a risk of data leakage. In [4], the author gives a language which permits to serve data with policies by agent; agent should prove their action and authorization to use particular data. In this logic data owner attach Policies with data, which contain a description of which actions are allowed with which data, but there is the problem of Continuous auditing of agent, but they provide solution that incorrect behavior. Should monitor and agent should give justification for their action, after that authority will check the justification. In [5], authors gives a three layer architecture which protect information leakage from cloud, it provides three layer to protect data, in first layer the service provider should not view confidential data in second layer service provider should not do the indexing of data, in third layer user specify use of his data and indexing in policies, so policis always travel with data. In [6], authors present accountability in federated system to achieve trust management. The trust towards use of resources is accomplished through accountability so to resolve problem for trust management in federated system they have given three layers architecture, in first layer is authentication and authorization in this authentication does using public key cryptography. Second layer is accountability which perform monitoring and logging [12]. The third layer is anomaly detection which detects misuse of resources. This mechanism requires third party services to observe network resources.

CONCLUSION

This paper presents effective mechanism, which performs automatic authentication of users 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 also able to know the duplication of data made without his knowledge. Data owner should not worry about his data on cloud using this mechanism and data usage is transparent, using this mechanism.

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 security of store data and to reduce log record generation time.

REFERENCES

1. Smitha Sundareswaran, Anna C. Squicciarini and Dan Lin, 2012. Ensuring Distributed Accountability for Data Sharing in the Cloud,", IEEE Transaction on Dependable a Secure Computing, 9(4): 556-568.
2. Pearson, S., Y. Shen and M. Mowbray, 2009. A privacy Manager for Cloud Computing, Proc. Int'l Conf. Cloud Computing (cloudcom), pp: 90-106.
3. Pearson, S. and A. Charlesworth, 2009. Accountability as a Way Forward for Privacy Protection in the Cloud, Proc First Int'l conf. Cloud Computing.
4. Corin, R., S. Etalle, J.I. Den Hartog, G. Lenzini and I. Staicu, 2005. A Logic for Auditing Accountability in Decentralized Systems, Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp: 187-201.
5. Squicciarini, A., S. Sundareswaran and D. Lin, 2010. Preventing Information Leakage from Indexing in the Cloud, Proc. IEEE Int'l Conf. Cloud Computing.
6. Chun, B. and A. C. Bavier, 2004. Decentralized Trust Management and Accountability in Federated System, Proc. Ann. Hawaii Int'l Conf. System Science (HICSS).
7. Crispo, B. and G. Ruffo, 2001. Reasoning about Accountability within Delegation, Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp: 251-260.
8. Kerana Hanirex, D. and K.P. Kaliyamurthie, 2013. Multi-classification approach for detecting thyroid attacks, International Journal of Pharma and Bio Sciences, 4(3): B1246-B1251.
9. Khanaa, V., K. Mohanta and T. Saravanan, 2013. Comparative study of uwb communications over fiber using direct and external modulations", Indian Journal of Science and Technology, 6(suppl 6): 4845- 4847.
10. Kumar Giri, R. and M. Saikia, 2013. Multipath routing for admission control and load balancing in wireless mesh networks, International Review on Computers and Software, 8(3): 779-785.
11. Kumaravel, A. and K. Rangarajan, 2013. Routing alogrithm over semi-regular tessellations, 2013 IEEE Conference on Information and Communication Technologies, ICT 2013.
12. Kumaravel, A. and K. Rangarajan, 2013. Algorithm for automaton specification for exploring dynamic labyrinths, Indian Journal of Science and Technology, 6(suppl 6).