IJRRECS/October 2013/Volume-1/Issue-6/1418-1422 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DATA SHARING ON ENTRUSTED STORAGE WITH ATTRIBUTE-BASED ENCRYPTION

G.Nani Babu[1], Balaji Loyisetti[2]

[1]M.Tech Student, Dept of CSE, Ramachandra College of Engineering & Technology, Eluru, A.P, India

Email: nanibabu553@gmail.com

[2]Associate Professor, Dept of CSE, Ramachandra College of Engineering & Technology, Eluru, A.P, India

Email: balucse504@gmail.com

ABSTRACT:

Cloud computing put up on established trends and offers a variety of services that can profit its customers, by means of providing quick access to their data, scalability, data storage, data recovery and guard against various hackers, and usage of the network and infrastructure conveniences for motivating the outlay exposed of the deliverance of services despite the fact that growing the speediness and suppleness with which services are organized. Along with the extensive enthusiasm on cloud computing, though, concerns on data security with cloud storage are arising due to unpredictability of the service and malicious attacks from hackers. Recently more and more proceedings on cloud service outage or server fraud with major cloud infrastructure providers are reported. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. Users' data are typically processed indistinctly, as in unknown machines users do not operate is a main feature of the cloud services. To make sure that any access to the data of users will set off validation and automatic logging local to the java archives and we persuade the JAR programmable abilities to equally generate an active and object of traveling. We also provide

distributed auditing methods to reinforce user's control. A novel approach, namely Cloud Information Accountability framework is proposed which is based on the idea of information accountability. The proposal of the Cloud Information Accountability structure presents widespread challenges, together with exclusively identifying cloud service provider.

Keywords: Cloud computing, Accountability, Data security, Java archives.

1. INTRODUCTION:

In the cloud computing structure, the elevated range of essential confidentiality and safety issues are due to the fact that users' data and applications exist in at least for a certain amount of time on the cloud cluster that is maintained by a third party [4]. The data processed on clouds are frequently outsourced and are important to issues related to responsibility, including the procedure of individually dedicated information [7]. Such doubts are becoming a considerable obstacle to an extensive acceptance of cloud service. Approaches of conventional access control were developed for closed domains in spread environments are not suitable. The data handling can be outsourced to other entities in the cloud by the direct cloud service provider and theses entities can also entrust the tasks to others [1]. An effectual mechanism was necessary to provide them that monitor the usage of user's data in the cloud which is shown in fig1. To promise suitable revelation of sensitive data among multiple users, fine-grained data access control mechanisms frequently need to be in place [9] [12]. A novel approach namely Cloud Information Accountability framework is proposed in this paper based on the concept of information accountability. The proposal of the Cloud Information Accountability structure presents widespread challenges, together with exclusively identifying cloud service provider. Remote data service providers are approximately certain to be outside the users' trust domain, and are not allowed to learn users' responsive information stored on their servers [3]. The usages of procedures attached to the data are proposed and present logic for responsibility data in disseminated settings. In remote data storage users do not actually own their data. Our basic approach toward addressing the issues by any entity in the cloud is to make longer the programmable potential of files of

Java Archives to log the usage of the data of user involuntarily [11]. With a central point of contact which forms a link between them and the user in order to cope with this issue, the Java Archives are provided.

2. METHODOLOGY:

We depend on image files by means of cloud computing because images represent a very common content type for end users and organizations and are increasingly hosted in the cloud as part of the storage services offered by the effectiveness computing standard is featured [5]. The users send their information as admission control policies and logging policies in the direction of cloud service provider's that they want to implement, enclosed in Java Archive files [14]. Our basic approach toward addressing the issues by any entity in the cloud is expanding the programmable potential of Java Archives to log the usage of the data of user involuntarily. Examination of whether a single logger component, used to grip more than one file, fallout in storage overhead. The usages of procedures attached to the data are proposed and present logic for responsibility data in disseminated settings [2]. The proposal of the Cloud Information Accountability structure presents widespread challenges, together with exclusively identifying cloud service provider. The decentralized logging mechanism meets the dynamic nature of the cloud but also imposes challenges on ensuring the integrity of the logging [8] [15]. To access the data, an automated mechanism of logging that is local to the Java Archives is triggered. Even when copies of the Java Archives are produced, the user includes managing over his data at any position as this strong binding exists [6]. With a central point of contact which forms a link between them and the user in order to cope with this issue, the Java Archives are provided. To address confidentiality concerns of end users and then develop a confidentiality manager, accountability mechanisms are proposed. As the user's private data are sent to the cloud in an encrypted form, the processing is done on the encrypted data and to make known the correct result, the output of the processing is unsure by the confidentiality manager who provides only partial features which does not assurance security [10]. For dealing with the continuous conviction administration in associated systems, a layered architecture is presented. Delegation is harmonizing at calculating the information workflow in the cloud. All the

way through cryptographic mechanisms, researchers have examined responsibility mostly as a demonstrable property [13].

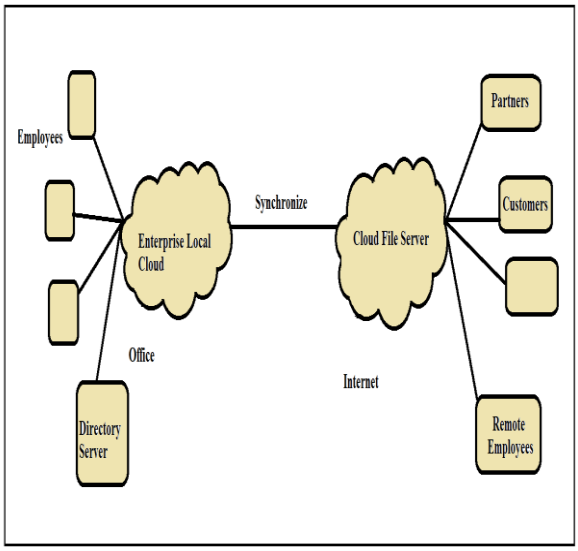

Fig1. An overview of Data Sharing in Cloud Computing

3. RESULTS:

The visual projection can happen at three points with respect to time such as: at some point in the confirmation, for the period of encryption of log records and for the period of the integration of the logs. Initially the time taken to produce a log file is examined and later measures the overhead in the system. With reverence to storage overhead our construction is very light and in that the only information to be accumulated are given by the definite files and the related logs. Examination of whether a single logger component, used to grip more than one file, fallout in storage overhead. Java Archives take action as a compressor of the files that it holds.

4. CONCLUSION:

Based on the idea of information accountability, a new methodology, namely Cloud Information Accountability outline is proposed. Cloud computing put up on established trends and offers a variety of services that can profit its customers, by means of providing quick access to their data, scalability, data storage, data recovery and guard against various hackers, and usage of the network and infrastructure conveniences for motivating the outlay exposed of the deliverance of services despite the fact that growing the speediness and suppleness with which services are organized. The proposal of the Cloud Information Accountability structure presents widespread challenges, together with exclusively identifying cloud service provider. A system is projected for a revolutionary advance along with an auditing system intended for reluctantly logging any admission to the data in the cloud. The revolutionary approach simultaneously with an auditing method is

proposed for logging involuntarily of several admissions to the data and allows the data owner to audit his content however besides execute well-built back-end protection if needed. In the direction of smoothing the progress of independent safeguard of traveling content in the long term a wide-ranging and additional general object-oriented method is designed. At providing software tamper resistance for java applications, the examination is aimed. To substantiate the reliability of the Java Running Environment and the confirmation of Java Archive files enhancement of our approach is planned in the future.

REFERENCES:

[1] E. Barka and A. Lakas, "Integrating Usage Control with SIP-Based Communications," J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

[2] B. Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.

[3] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies, pp. 1-14, 2009.

[4] OASIS Security Services Technical Committee, "Security Assertion Markup Language (saml) 2.0," http://www.oasis-open.org/committees/tc home.php?wg abbrev=security, 2012.

[5] X. Feng, Z. Ni, Z. Shao, and Y. Guo, "An Open Framework for Foundational Proof-Carrying Code," Proc. ACM SIGPLAN Int'l Workshop Types in Languages Design and Implementation, pp. 67-78, 2007.

[6] D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology, pp. 213-229, 2001.

[7] Y. Chen et al., "Oblivious Hashing: A Stealthy Software Integrity Verification Primitive," Proc. Int'l Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.

[8] R. Bose and J. Frew, "Lineage Retrieval for Scientific Data Processing: A Survey," ACM Computing Surveys, vol. 37, pp. 1-28, Mar. 2005.

[9] S. Etalle and W.H. Winsborough, "A Posteriori Compliance Control," SACMAT '07: Proc. 12th ACM Symp. Access Control Models and Technologies, pp. 11-20, 2007.

[10] P. Ammann and S. Jajodia, "Distributed Timestamp Generation in Planar Lattice Networks," ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.

[11] P. Buneman, A. Chapman, and J. Cheney, "Provenance Management in Curated Databases," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD '06), pp. 539-550, 2006.

[12] 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.

[13] B. Chun and A.C. Bavier, "Decentralized Trust Management and Accountability in Federated Systems," Proc. Ann. Hawaii Int'l Conf. System Sciences (HICSS), 2004.

[14] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. ACM Conf. Computer and Comm. Security, pp. 598- 609, 2007.

[15] F. Martinelli and P. Mori, "On Usage Control for Grid Systems," Future Generation Computer Systems, vol. 26, no. 7, pp. 1032-1042, 2010.