IJRRECS/October 2013/Volume-1/Issue-6/1435-1440 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

LIABILITY FOR DATA DISTRIBUTION IN CLOUD COMPUTING

B.Navaneetha[1], B.Madhavi Devi[2], Ch.Srinivasulu[3]

[1]Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

[2]Assistant Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

[3]Associate Professor, Dept of IT, J.B. Institute of Engineering & Technology, Hyderabad, A.P, India

ABSTRACT:

Fine-grained data access control mechanisms frequently need to be in place to promise suitable revelation of sensitive data among multiple users. Even though still at its early stage, Cloud Computing has before now drawn great consideration, and its advantages have attracted an increasing number of users to outsource their limited data centers to remote cloud servers. Disclosure of responsive information, stored on remote data a server has to be severely protected earlier to users has autonomy to use the data services. Users' data are typically processed distantly, as in unknown machines users do not operate is a major feature of the cloud services. A novel approach, namely Cloud Information Accountability framework is proposed which is based on the idea of information accountability. Contrasting from privacy protection knowledge, information responsibility focuses on keeping the data usage clear and track able. To make sure that any admission to users' data will trigger validation and automatic logging local to the java archives and we persuade the java archive programmable abilities to create a dynamic object. An object-centered approach is proposed so that it facilitates by including our logging method together with users' data and strategy.

Keywords: Cloud Computing, Multiple users, Cloud Information Accountability, Java archives.

1. INTRODUCTION:

Cloud computing, regarded as the potential IT structural design, and even promises to make available unlimited and elastic storage resource as a service to cloud users in an incredibly cost eventual way. Current advances in IT have greatly made possible remote data storage and sharing. New applications such as online social networks and online documents make available very expedient ways for people to accumulate and share a variety of data including personal profile, electronic documents on remote online data servers [4]. Even though still at its early stage, Cloud Computing has before now drawn great consideration, and its advantages have attracted an increasing number of users to outsource their limited data centers to remote cloud servers. Data protection is a serious concern for remote data storage. On one hand, disclosure of responsive information, such as health records, stored on remote data servers has to be severely protected previous to users have autonomy to use the data services [9]. Fine-grained data access control mechanisms frequently need to be in place to promise suitable revelation of sensitive data among multiple users. Based on the notion of information accountability a novel approach namely Cloud Information Accountability framework is proposed in this paper. Concerns arise since in the cloud computing is not always clear to individuals as their personal information is requested or passed on to other parties [2]. On the other hand, in remote data storage users do not actually own their data. 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 [11]. Cloud computing has elevated a range of essential confidentiality and safety issues. In the cloud computing such 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 which is owned and maintained by a third party [14].

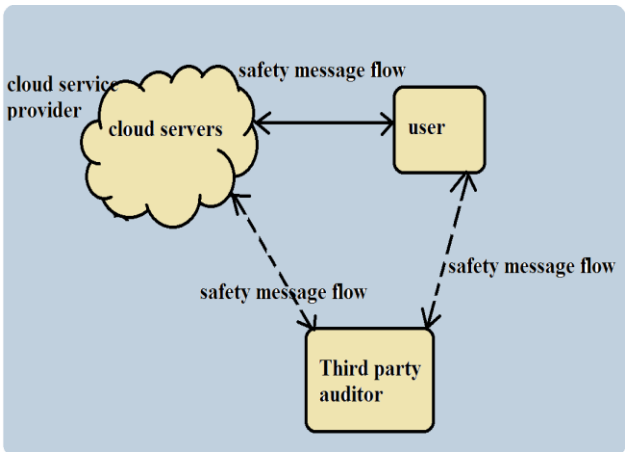

Fig 1: Sharing of information in Cloud Computing

2. METHODOLOGY:

We build up two different modes for auditing known as push mode and pull mode which are associated with the accountability feature. The pull mode refers to another approach whereby the user can regain the logs as needed and the push mode refers to logs being occasionally sent to the data owner or stakeholder [3] [7]. Adapting to a highly decentralized infrastructure the design of the Cloud Information Accountability framework presents extensive challenges, including exclusively identifying cloud service provider ensuring the consistency of the log etc. By any entity in the cloud our basic approach toward addressing these issues is to leverage and extend the programmable capability of Java Archives files to automatically log the usage of the users' data [12]. To cloud service provider's users will send their data shown in fig1 along with any policies such as admission control policies and logging policies that they want to implement, enclosed in Java Archive files [5]. An automated and authenticated logging mechanism local to the Java Archives are triggered to access the data. The user includes managing over his data at any position as this strong binding exists even when copies of the Java Archives are created. On ensuring the integrity of the logging, such decentralized logging mechanism meets the dynamic nature of the cloud but also imposes challenges [1] [6]. We provide the Java Archives with a central point of contact which forms a link between them and the user in order to cope with this issue. To monitor the loss of any logs from any of the Java Archives this allows and records the error correction information sent by the Java Archives [15]. Moreover, any access to its enclosed data will be denied if a Java Archive is not able to contact its central point. At present, by means of cloud computing we center on image files 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. Accountability mechanisms are proposed to address confidentiality concerns of end users and then develop a confidentiality manager. The processing is done on the encrypted data as the user's private data are sent to the cloud in an encrypted form [10]. To reveal the correct result the output of the processing is unsure by the confidentiality manager. However,

the confidentiality manager provides only partial features in that it does not assurance security once the data are being disclosed. A layered architecture is presented for addressing the end-to-end trust management and responsibility problem in associated systems. Researchers have examined responsibility mostly as a demonstrable property through cryptographic mechanisms [13]. The usages of procedures attached to the data are proposed and present logic for responsibility data in disseminated settings. Similarly, logic for designing accountability-based distributed systems is proposed. In this paper, an interesting approach related to accountability in case of delegation is proposed. Delegation is complementary to our work, in that we do not aim at calculating the information workflow in the cloud. An agent-based system specific to grid computing is proposed [8]. Distributed jobs, along with the resource consumption at local machines are tracked by static software agents.

3. RESULTS:

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. Initially the time taken to produce a log file is examined and later measures the overhead in the system. By means of reverence to time the visual projection can happen at three points: at some point in the confirmation, for the period of encryption of log records and for the period of the integration of the logs. Java Archives take action as a compressor of the files that it holds. Examination of whether a single logger component, used to grip more than one file, fallout in storage overhead.

4. CONCLUSION:

Cloud Computing has before now drawn great consideration, and its advantages have attracted an increasing number of users to outsource their limited data centers to remote cloud servers. A novel approach, namely Cloud Information Accountability framework is proposed which is based on the idea of information accountability. The pioneering approach simultaneously with an auditing method is proposed for involuntarily logging any access to the data in the cloud and allows the data owner to audit his content however besides execute well-built back-end protection if needed. For reluctantly logging any admission to the data in the cloud, a system is projected for a

revolutionary advance along with an auditing system. To confirm the reliability of the Java Running Environment and the confirmation of Java Archive files improvement of our approach is planned in the future. To smooth the progress of independent safeguard of traveling content in the long term a wide-ranging and additional general object-oriented method is designed. The examination is aimed at providing software tamper resistance for java applications.

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] Flickr, http://www.flickr.com/, 2012.