Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 11, November 2015, pg.289 – 294

RESEARCH ARTICLE

TRACKING OF USER INFORMATION IN CLOUD ENVIRONMENT

[1]M.Phani Anusha (M. Tech Student), **[2]N.L.Prasanna** Asst. Prof
(Vignan's Lara Institute of Technology & Science, Guntur)
Phanianusha32@gmail.com, prasanna.manu@gmail.com

ABSTRACT:

A cloud computing present a pioneering means to balance the present spending and deliverance representation and provides scalable and regularly virtualized assets as a service. Users can dread of losing control of their own data and can become a considerable obstacle to the wide acceptance of cloud services. Accountability mechanisms are introduced to address confidentiality concern of end client and subsequently build up a confidentiality manager. System of cloud information accountability was introduced to carry out automatic logging and dispersed auditing of significant access performed by any individual, achieved at any time at any provider of cloud service. To defend against attacks carry out on offline java achieves, the cloud information accountability comprise a log harmonizer containing two main tasks: to deal copies of java achieves and to get well corrupted logs.

Keywords: Java achieves, Cloud service, Cloud information accountability, Log harmonizer.

1. INTRODUCTION:

Cloud computing has elevated a range of essential confidentiality and safety issues. In the cloud computing such concerns are due to reality that users' data and applications exist in at least for a certain amount of time on cloud cluster which is preserved by a third party [4]. Researchers have examined responsibility mostly as a demonstrable property through

cryptographic mechanisms. The usages of procedures attached to the data are introduced and present logic for responsibility data in disseminated settings. Similarly, logic for designing accountability-based distributed systems is introduced. Foremost to a number of concerns related to responsibility and data practiced on clouds are regularly outsourced. To the wide acceptance of cloud service such fears are becoming an important obstacle. It is necessary to provide an efficient mechanism for them to supervise the usage of user's data in the cloud. Accountability mechanisms are introduced to address confidentiality concern of end client and subsequently build up a confidentiality manager [8]. A novel highly decentralized information liability framework is introduced to keep track of the authentic procedure of user information within cloud. An object-centered approach is introduced so that it makes possible by including our logging method together with users' data and policies. To make sure that any accession to client information will set off regular logging to java achieves [1]. Processing is made on encrypted information as the user's confidential information is send to cloud in an encrypted structure. In the direction of revealing correct result output of processing is deobfuscated through confidentiality manager. However, the confidentiality manager provides only partial features in that it does not assurance security once the data are being disclosed.

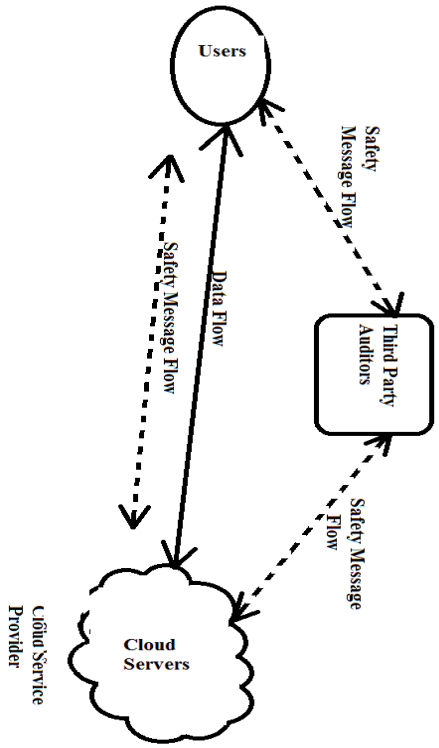

Fig1: An overview of data sharing in Cloud Computing.

2. METHODOLOGY:

Cloud computing presents an innovative way to balance the present spending and deliverance representation in support of IT services and also provides scalable and regularly virtualized assets as a service. Specified service details are distracted from user who no longer necessitates being proficient of knowledge infrastructure. Equipment which fundamentally route and host their data is not known by the users. Users also start upsetting about losing control of their own data while enjoying the simplicity brought by this new technology [11]. Users' data are typically processed vaguely, as in unidentified machines client do not function is most important feature of the cloud services. Users can dread of losing control of their own data and can become a considerable obstacle to the wide acceptance of cloud services. A variety of receptive data shared in the cloud demands the cloud data distribution service to be accountable for dependable enforcement concerning data content accession between possible users in support of data holder [3] which is shown in Fig 1. We have to rearrange the problem of access control in this open environment since cloud server might no longer be in comparable faith domain as the data owners, where cloud server receive complete charge of organization of outsourced information however are not inevitably trusted regarding data privacy. A layered architecture is obtainable for tackling the continuous trust managing and responsibility problem in associated systems [14]. Concern occurs since in cloud computing is not always clear to individuals as their personal information is requested or passed on to other parties. The Cloud Information Accountability structure introduced carry out automatic logging and dispersed auditing of significant access performed by any individual, achieved at any time at any provider of cloud service [9]. There are two main components i.e. logger which is powerfully joined with the user's information, so that it is downloaded when the information are accessed, and is copied whenever the information are copied. It holds a particular request or copy of the user's data and is accountable for logging accession to copy. Log harmonizer outlines necessary constituent allows the user to use to the log files [7]. The logger is powerfully joined with user's information. Its foremost tasks include involuntarily logging accession toward data items that it enclose and by encrypting log record by means of public key concerning substance possessor, and occasionally distributing them towards harmonizer of log [2]. It is configured toward making sure that access and usage control policies linked with the data are privileged. The logger is also accountable for producing the error improvement information in support of every log record and transmits identical to the log harmonizer. The error alteration data joined with the

encryption and validation mechanism provides an active and reliable recovery mechanism [16]. The log harmonizer produces the master key being the expected component and it holds decryption key in support of IBE key pair, since it is accountable for decrypting the logs. On the other hand, the decryption can be approved on user end when path among log harmonizer as well as user is not believed [12]. The logger needs only minimal support from the server in order to be organized. The rigid combination connecting data besides logger, consequence in extremely dispersed logging system by meeting our first design requirement. Additionally, the logger is not installed on system as it is not very disturbing in its actions and thus by satisfying our requirement. Delegation is complementary to effort, in which we do not intend at calculating the information workflow in the clouds [5]. An agent-based scheme detailed toward grid computing is introduced. Innovative approaches together with an auditing mechanism for involuntarily logging any accession to data in cloud were introduced. Introduced system not only allows the data title-holder to review his content but also execute strong back-end safety if needed and allows the data holder to review copies of its information that were prepared devoid of his knowledge [15]. In the future, to authenticate reliability of java running environment and confirmation of java achieve plan to refine it. For java appliances this investigation is aimed at providing software obstruct resistance. In the long term, to make possible independent fortification concerning traveling content, we plan to intend a wide-ranging and additionally general object-oriented system [10]. Dispersed jobs, all along with resource utilization at local machines are followed by fixed software agents. The concept of responsibility policies is mostly focused on resource utilization and on following of sub jobs practiced at numerous computing nodes, to a certain extent than accession manages. The main accountability of the outer java achieve is to hold verification of entities which want to admission data accumulated in java achieve file. Data holder may not identify the accurate cloud service provider that is going to hold the information [6]. Confirmation is particular consistent with the server functionality sooner than the server individuality. Each internal java achieve contains encrypted information, class files to make easy recovery of log files and put on show sheltered data in an appropriate arrangement and a log file in support of every encrypted item. Pure Log records each access towards data. The log files are employed for pure auditing function. Access Log has two tasks such as logging and implements access control. When access demand is denied, the java achieve will evidence the occasion when request is prepared [13]. When access demand is approved, the java achieves will evidence access information all along duration for which access is authorized. To defend against attacks carry out on offline java achieves, the cloud

information accountability comprise a log harmonizer containing two main tasks: to deal copies of java achieves and to get well corrupted logs. Every log harmonizer is in accusation of copies concerning logger components enclosing similar set of data objects. The harmonizer is put into practice as a java achieve file which does not contain user's information items being reviewed.

3. RESULTS:

The Cloud Information Accountability structure introduced carry out automatic logging and dispersed auditing of significant access performed by any individual, achieved at any time at any provider of cloud service. With reverence to storage overhead, introduced construction is very light and in that the only information to be accumulated are given by the definite files and the related logs. 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. Examination of whether a single logger component, used to grip more than one file, fallout in storage overhead.

4. CONCLUSION:

Innovative approaches together with an auditing mechanism for involuntarily logging any accession to data in cloud were introduced. An approach related to accountability concerning delegation is introduced which is highly decentralized information liability framework to keep track of the authentic procedure of user information within cloud. Introduced system not only allows the data title-holder to review his content but also execute strong back-end safety if needed and allows the data holder to review copies of its information that were prepared devoid of his knowledge. The main accountability of the outer java achieve is to hold verification of entities which want to admission data accumulated in java achieve file.

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] "Ensuring Distributed Accountabilityfor Data Sharing in the Cloud", Smitha Sundareswaran, Anna C. Squicciarini, and Dan Lin, 2012

[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.

[16] 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.

