Efficient and Protected CIA Framework for Data Sharing in the Cloud

Mr. Prasad P Kharade[1] Prof. S. B. Natikar[2]
[1]Student of M.E [2]Assistant Professor
[1,2]Department of Computer Engineering
[1,2]VACOE

Abstract— Cloud computing is the technique that offers us various kinds of services to be used via internet. There are two types of computing sources such as software and hardware. For a client it enables more accessibility of services that can accessed by demand via internet .Cloud computing offers a major feature like unknown service location and that is becoming the challenging task in cloud computing. To overcome this problem CIA (cloud information accountability) framework can be used that records programmed logging and auditing to every access to the data and by introducing the steganography concept the user details get tracked so in this way increasing the security of data.

Key words: cloud computing, data sharing, security

I. INTRODUCTION

The secure CIA (cloud information accountability) framework that have introduced performs programmed logging to the data and also conducts the distributed auditing of every access that is done by any unit or by any user, that is in use out at any point of time at any csp. This structure contains the two important mechanism logger and log harmonizer. we have the JAR file and JAR file contains a group of some simple access control rules like read, write and copy etc that tells us that whether and how the cloud services and other entity's and companies are permitted to get in touch with the content itself and beyond that we are going to check the openness of the JRE on the system on which the logger components is present. While enjoying all the remuneration of the services that is given by this innovative expertise users also begin embracing with reference to losing the be in command of their personal data because user's data behavior out in the cloud is a bit puzzling because user don't be familiar with that on what machines data will get processed and .users recognize that the data processed on cloud are often catch out and the most vital to a number of issues linked accountability, and it contains the managing of individually personage information or entity's undisclosed information. Such kinds of uncertainties produces to some problems like there is more adoption of the user's personal data to other cloud service provider and such type of the trustworthiness and are going to check by the concept of oblivious hashing. The given tactic will also responsible for the JAR file by converting the JAR file into obfuscated code means the code which makes the communication baffling and in this way by means of obfuscation provides some more layer of safety to the infrastructure that will profit us a lot. spaced out from that we are going to broaden the security of users' records by provable data possessions for honesty verification. Based on the prototype settings that have clear at the time of creation, the JAR file provides us some of the handling power means how data is going to used and pairing it with logging, or will give only logging functionality. As it states that on every occasion there is a logging for any data the JAR will involuntarily generates a log record that comprise all the particulars of logging or accessing of content and for each access to the content or data that will tell the data owner about with the admittance means who have accessed the data and how many times the exacting user has accessed the data. In existing system the cloud computing is the liberation of computing as a service rather than a product by which unrestricted possessions, software and information are specified to computers and other devices as service like the electricity grid over a network. In these days a single server deals with the plentiful wishes from the user. Here the server has to take effort for both the request from the user simultaneously, so the dealing out time will be more. To alleviate users concerns it is very vital that to suggest well-organized way for users so that user can administer and can trail that the real usage of the information that will assist them for generating log files that contains all essential information. For instance users are mandatory to be able to assurance that their data are going to truly handled according to anything the service rank agreements with the intention of user has made at the time they sign on for services. so in this way projected a innovative CIA i.e cloud information accountability skeleton that will take charge of the genuine usage of data and simultaneously give the details of all data or produce a log evidences with every admission to the user and other data stakeholders and overtake this logs to the data owner so that data owner can follow the authentic procedure of their own data so in this way are civilizing the data's security. In this paper[7] by including the frankness checks and oblivious hashing[14] skill in order to construct up the reliability of our system in case of compromised JRE and updating every part of the log account formation to offer additional guarantees of integrity. and genuineness and increasing the security investigation to face more feasible assault scenarios. A JAR file is idea that is in use from the Java language.JAR means JAVA Achieve and it is particularly used to maintain all the files in only one folder by compressing their duration instead of care files unconnectedly in this way we are saving the memory by using JAR. The JAR file includes a set of trouble-free admission control policy that tells us that whether and how the cloud servers and probably other users and other entities are permissible or sanctioned to right to use the data or content itself. Finally when all the verification got finished then, the service donor will get access to access the data from the JAR file. So it is in reality depends upon the whatsoever arrangement settings have been clear at the time of creation, the JAR file will provides usage manage linked with the logging, or will provide only logging functionality. As for the logging, every time there is an access to the data, then JAR file will automatically create a log record.

II. SURVEY

Cloud computing has introduced a number of the significant confidentiality and security issues. a quantity of issues are

due to reasons, in the cloud system what happens usually the users data and some applications will get reside at least for a definite quantity of time on the cloud sever and such devices are away of control from the user and which is completely owned and maintained by a third party. some issue arises as in the cloud machinery it is not forever obvious to anybody or no one can tell that why their individual or secret information is asked and how that information will be used during or to whom that information will be sent .Up till now, small work has been ended in this particular scope, in particular with reverence to accountability. They have predictable accountability device to tackle confidentiality issues of end users and then develop a isolation manager. so The basic idea is that the users secretive data will get sent to the clouds in an encrypted type so that no one can tacit the content itself, and the all dealing out on data that will be done on the encrypted data .Here, whatsoever the output that are receiving that will be the deobfuscated by the privacy manager to shows the accurate result. However, the privacy manager provisions only little amount of features in that it does not promise the defense once the data are being open to a different user. The authors are presenting the covered design for viewing the end-to-end faith supervision and responsibility troubles in federated systems [7]. The authors center of attention is very dissimilar as of ours, in that they mostly manage faith associations for account ability, along with validation and irregularly detection. Further, their clarification requires an extra trusted party service to entire the monitoring and focuses on minor stage monitoring of structure resources. Researchers have investigated liability regularly as a verifiable property during cryptographic mechanisms, chiefly in the context of electronic commerce.

III. PROPOSED SYSTEM

In planned system the negative aspect of existing system will be overcome. stegenography means it is a technique of embedding an supplementary information into the digital contents, that is unnoticeable to viewers so on every occasion an user downloading data from web site, user details(i.e username or etc) will be concealed with the downloaded data using this steganography method so that, if the data owner found that his data altered anywhere means they can with no trouble identifies the user particulars who leaked the data by retrieving steganography details. In this procedure by providing the choice to data owners for uploading file or remove file by online by given that set of authentication(like OTP, CAPTCHA, etc). Whenever a data downloaded by any entity, that user particulars will be buried within the data termed technically as Steganography. its major exercise is to trace the user who is using the data in illegal places. In this way in planned scheme we are incorporating least significant Bit stegenography method. The proposal at the back of the LSB algorithm is to put in the bits of the concealed meaning into the least significant bits of the pixels.

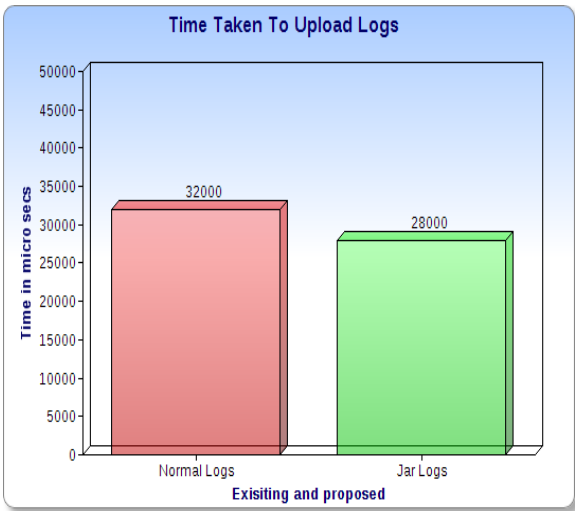

Fig. 1: Result

In above graph it is clear that the dissimilarity between existing system and planned system in the terms of normal logs and jar logs. In the normal logs the time taken to upload the files is more as compared to the jar files

IV. CONCLUSION

This section includes that what we can conclude from our Secure CIA architecture. Here, We have expected revolutionary approaches for mechanically cataloguing to any access to the data in the cloud with adding .we have provided logging mechanism with auditing that will benefits us a lot. This system allows the data owner to not only review his content but also it is going to provide physically powerful back-end safety and one of the main features of our secure structural design is that it enables the data owner to review even if those copies of its data were made exclusive of his knowledge and by using the stegenography idea a strong security is linked with the user's data. In this way stegenography is used to trace the user who has unofficial access to the data in this way it provides strong security to this architecture.

V. FUTURE SCOPE

In the future, we are setting up to progress our secure structural design to authenticate the honesty of the JRE and the validation of JARs. We are also setting up to design a broad and more nonspecific object-oriented approach that will offer us the independent defense to the traveling information or data. We also interested to provide the support to different types of security policies.

REFERENCES

[1] P. Ammann and S. Jajodia, Distributed Timestamp Generation in Planar Lattice Networks, ACM Trans. Computer Systems, vol. 11, pp. 205-225, Aug. 1993.
[2] 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.
[3] E. Barka and A. Lakas, Integrating Usage Control with SIP-Based Communications, J. Computer Systems, Networks, and Comm., vol. 2008, pp. 1-8, 2008.

[4] D. Boneh and M.K. Franklin, Identity-BasedEncryption from the Weil Pairing, Proc. Intl Cryptolog Conf. Advances in Cryptology, pp. 213-229, 2001.
[5] R. Bose and J. Frew, Lineage Retrieval for Scienti_c Data Processing: A Survey, ACM Computing Surveys, vol. 37, pp. 1- 28, Mar. 2005.
[6] P. Buneman, A. Chapman, and J. Cheney, Provenance Management in Curated Databases, Proc. ACM SIGMOD Intl Conf. Management of Data (SIGMOD 06), pp. 539-550, 2006.
[7] B. Chun and A.C. Bavier, Decentralized Trust Management and Accountability in Federated Systems, Proc. Ann. Hawaii Intl Conf. System Sciences (HICSS), 2004.
[8] W. Lee, A. Cinzia Squicciarini, and E. Bertino, The Design and Evaluation of Accountable Grid Computing System, Proc. 29th IEEE Intl Conf. Distributed Computing Systems (ICDCS 09), pp. 145-154, 2009.
[9] J.H. Lin, R.L. Geiger, R.R. Smith, A.W. Chan, and S. Wanchoo, Method for Authenticating a Java Archive (jar) for Portable Devices, US Patent 6,766,353, July 2004.
[10] F. Martinelli and P. Mori, On Usage Control for Grid Systems, Future Generation Computer Systems, vol. 26, no. 7, pp. 1032-1042, 2010.
[11] J. Park and R. Sandhu, The Uconabc Usage Control Model, ACM Trans. Information and System Security, vol. 7, no. 1, pp. 128- 174, 2004.
[12] S. Pearson and A. Charlesworth, Accountability as a Way Forward for Privacy Protection in the Cloud, Proc. First Intl Conf. Cloud Computing, 2009
[13] A. Pretschner, M. Hilty, F. Schuo tz, C. Schaefer, and T. Walter, Usage Control Enforcement: Present and Future, IEEE Security Privacy, vol. 6, no. 4, pp. 44-53, July/Aug. 2008.
[14] Y. Chen et al., Oblivious Hashing: A Stealthy Software Integrity Veri_cation Primitive, Proc. Intl Workshop Information Hiding, F. Petitcolas, ed., pp. 400-414, 2003.
[15] S. Miller, Use of Elliptic Curves in Cryptography, H. C. Williams, Ed., Advances in Cryptology CRYPTO, LNCS, vol. 218, 1985, Springer-Verlag, 1986, pp. 41726.
[16] G.Barthe,FedericoOlmedo,S.Z.Beguelin"Veri_able Security of Boneh-Franklin Identity-Based Encryption"

