International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Shared Ascendancy Predicated Privacy-preserving Authentication Protocol on Cloud Data

Mohd Abdul Aziz Rahaman[1]& N. Srinivas[2]
[1]M-Tech Dept. of CSE,VignanaBharathi Institute of Technology, Hyderabad
[2]Associate Professor Dept. of CSE,VignanaBharathi Institute of Technology, Hyderabad

Abstract:

This paper discusses the current quandary faced in the cloud computing with regard to preserving the privacy in sharing the data. Cloud computing offers set of accommodations and resources utilizing internet. These accommodations are provided from data centers which are located throughout the world. Contemporary business models for organizations to deploy IT accommodations are offered by cloud computing without any upfront investment. Cloud computing simplifies providing the virtual resources from anywhere in the world to anywhere in the world via internet. With the immensely colossal-scale adoption of cloud computing, security issues are the main challenges which are need to be solved efficiently and efficaciously. The proposed system provides a solution for preserving the data in cloud with the avail of encryption protocol. Three modules are presented here namely data owner, Third Party Administrator, and retailer. Advanced Encryption Standard algorithm is implemented in the current work for encrypting the data which has to be stored in the cloud. This data can be retrieved by retailer on providing the valid signature key to decrypt the data.

Index terms: - Data storage; privacy preserving; public audit ability; cloud computing; TPA

1. INTRODUCTION

Cloud computing enables highly scalable accommodations to be facilely consumed over the Internet on an as-needed substructure. A consequential benefit of the cloud accommodations is that users' data are conventionally processed remotely in unknown machines that users do not possess or use. While relishing the accomodationbrought by this technology, users' get trepidacious of missing their data. It can become a consequential barrier to the wide adoption of cloud accommodations. A novel highly distributed information accountability framework to keep track of the genuine utilization of the users' data in the cloud. We introduce an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We influence the JAR coding capabilities to both engender a dynamic and moving object, and to ascertain that any access to users' data will trigger authentication and automated logging local to the JARs. To make the user's control more vigorous, we provide distributed mechanisms for auditing. We provide widespread experimental studies that demonstrate the efficiency and efficacy of the proposed approaches. It is typically a type of computing that relies on sharing computing resources rather than having local servers or personal contrivances to handle applications. In cloud computing, the word cloud (additionally phrased as "the cloud") is utilized as a metaphor for "the Internet," so the phrase cloud computing

denotes "a type of Internet-predicated computing," where different accommodations such as servers, storage and applications are distributed to an organization's computers and contrivances through the Internet. When compared to grid computing, a computing type where processing cycles that are unutilized for all computers in a network are harnesses to solve quandaries too intensive for any stand-alone machine. The applications are Sizablyvoluminous Data Analytics. Cloud computing is a type of computing where unutilized processing cycles of all computers in a network are harnesses to solve quandaries too intensive for any stand-alone machine.

2. RELATED WORK

Literature survey is the most paramount step in software development process. Afore developing the implement it is indispensable to determine the time factor, economy n company vigor. Once these things r satiated, ten next steps are to determine which operating system and language can be utilized for developing the implement. Once the programmers start building the implement the programmers need lot of external support. This fortification can be obtained from senior programmers, from book or from websites. Afore building the system the above consideration are taken into account for developing the proposed system.

Subsisting System:

However, most antecedent researches fixate on the authentication to realize that only a licit utilizer can access its sanctioned data, which ignores the case that different users may want to access and apportion each other's sanctioned data fields to achieve productive benefits. When a utilizer challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access sanctions. In this work, we aim to address a user's sensitive access desire cognate privacy during data sharing in the cloud environments, and it is paramount to design a humanistic security scheme to simultaneously achieve data access control, access ascendancy sharing, and privacy preservation. Precedent System does not have the option of granting/revoking data access

Proposed System:

In this paper, we address the aforementioned privacy issue to propose a shared ascendancy predicated privacy preserving authentication protocol (SAPA) for the cloud data storage, which realizes authentication and sanction without compromising a user's private information. The main contributions are as follows. Identify an incipient privacy challenge in cloud storage, and address a subtle privacy issue during a utilizer challenging the cloud server for data sharing, in which the challenged request itself cannot reveal the user's privacy no matter whether or not it can obtain the access ascendancy. Propose an authentication protocol to enhance a user's access request cognate privacy, and the shared access ascendancy is achieved by incognito access request matching mechanism. Apply cipher text-policy attribute predicated access control to realize that a utilizer can reliably access its own data fields, and adopt the proxy re-encryption to provide temp sanctioned data sharing among multiple users. Here we proposed the secured system and data owner can decide whether the utilizer can access the system or not.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

3. IMPLEMENTATION

Owner Registration:

In this module an owner has to upload its files in a cloud server, he/she should register first. Then only he/she can be capable of doing it. For that he requires to fill the details in the registration form. These details are maintained in a database.

Owner Authenticate:

In this module,any of the above mentioned person have to authenticate,they should authenticate by giving their emailid and password .

Utilizer Registration:

In this module if a utilizer wants to access the data which is stored in a cloud, he/she should register their details first. These details are maintained in a Database.

Utilizer Authenticate:

If the utilizer is a sanctioned utilizer, he/she can download the file by utilizing file id which has been stored by data owner when it was uploading.

Access Control:

Owner can sanction access or gainsay access for accessing the data. So users can able to access his/her account by the corresponding data owner. If owner does not sanction, utilizer can't able to get the data.

Encryption & Decryption:

Here we are utilizing this aes_encrypt&aes_decrypt for encryption and decryption. The file we have uploaded which has to be in encrypted form and decrypt it

File Upload:

In this module Owner uploads the file(along with meta data) into database, with the avail of this metadata and its contents, the cessation utilizer has to download the file. The uploaded file was in encrypted form, only registered utilizer can decrypt it.

File Download:

The Sanctioned users can download the file from cloud database.

Cloud Accommodation Provider Registration:

In this module, if a cloud accommodation provider (maintainer of cloud) wants to do some cloud offer , they should register first.

Cloud Accommodation Provider Authenticate:

After Cloud provider gets authenticated in, He/ She can optically discern Cloud provider can view the files uploaded by their clients. Withal upload this file into separate Cloud Database

TTP (trusted third party) authenticate:

In this module TTP has monitors the data owners file by verifying the data owner's file and stored the file in a database .Also ttp checks the CSP(CLOUD ACCOMMODATION PROVIDER),and ascertain whether the csp is sanctioned one or not.

4. EXPERIMENTAL RESULTS

Fig:-1 New User Registration

Fig:-2 Secure Login

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Fig:-3 Data Upload In Cloud

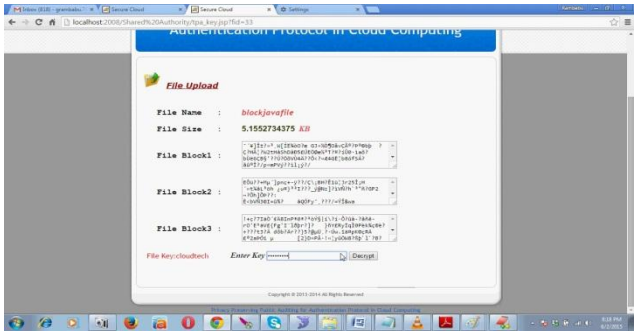

Fig:-4 Block Dividing

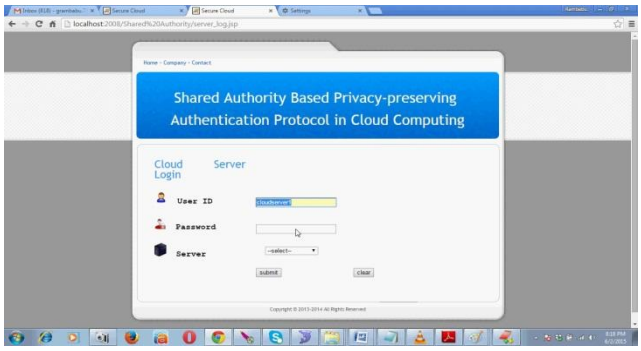

Fig:-5 Cloud Server Login

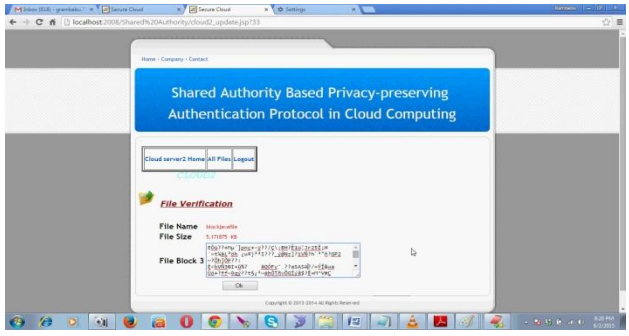

Fig:-6 File Verification

Fig:-7 Result

5. CONCLUSION

In this work, we have identified an incipient privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access ascendancy sharing. Authentication is established to assure data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. Utilizer privacy is enhanced by innominate access requests to privately apprise the cloud server about the users' access desires. Forward security is realized by the session identifiers to obviate the session correlation. It designates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

6. REFERENCES

[1] Privacy-Preserving Public Auditing for Secure Cloud Storage Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, IEEE Transactions On Computers, Vol. 62, No. 2, February 2013

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage

Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Comput- ing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.WANG Et Al.:Privacy-Preserving Public Auditing For Secure Cloud Storage 373

[4] International Journal of Computer Trends and Technology (IJCTT) - volume4Issue4 –April 2013 ISSN: 2231-2803 Http://www.ijcttjournal.org Page 828

[5] Privacy preserving public auditing system for data storage security in Cloud ComputingG.RajaMohan1, K.VenkataRaju

[6] Y. Zhu , H. Hu , G. Ahn and M. Yu "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage", IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp.2231 -2244 2012

[7] H. Wang "Proxy Provable Data Possession in Public Clouds", IEEE Trans. Services Computing, vol. 6, no. 4, pp.551 -559 2012 [online] Available:

[8] K. Yang and X. Jia "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Trans. Parallel and Distributed Systems, vol. 24, no. 9, pp.1717 -1726 2013 [online] Available:

[9] Q. Wang , C. Wang , K. Ren , W. Lou and J. Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp.847-859 -25 2011

[10] C. Wang , K. Ren , W. Lou and J. Li "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network, vol. 24, no. 4, pp.19 - 24 2010