IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Secured Data Sharing for Accountable Cloud

Basavaraj Chunchure[1] and Dr. Seetharam. K[2]
Associate Professor, Department of CSE[1]
Professor, Department of CSE[2]
Vignan's Institute of Management and Technology for Women, Hyderabad, India[1]
R.L Jalappa Institute of Technology, Doddaballapura, Karnataka, India[2]

Abstract: *Cloud computing is the latest computing paradigm that enables scalable and convenient resource sharing over the internet. It aims to provide computing as a utility over the internet on an as-needed basis. The advantage of this technology comes with various privacy and security risks. This can be a barrier to the larger acceptance of cloud based services. Solutions to the privacy come with the reintroduction of element of control and that is where the term accountability emerges. Accountable cloud can be the way to avoid various privacy issues. Even though there can be security risks associated especially with the sharing of data in such a highly dynamic and complicated environment. The proposed system will provide an additional client side verification for each outsourcing in order to enhance the client side security of data and thus provides an additional protection. Usually this verification is generally equipped with an additional step for checking every access from cloud service providers. As a whole the proposed system can provide the required accountability and secured data sharing using some simple methods and can increase the wider adoption of cloud based services without any fear of risks like data loss*

Keywords: Accountable cloud computing, Secure data sharing, Access control

I. INTRODUCTION

Cloud computing has gained wider attention in the recent years. Cloud computing provides a shared pool of services, including the data storage space, computing power, and other specialized corporate and user applications. The ability of the users to scale dynamically the IT operations without making many expensive and huge investments is the major attraction of cloud computing services. Cloud computing has got special characteristics that distinguish it from classical resource provisioning environments. It is more or less reliable and scalable and it provides services in the form of platform, infrastructure and applications. The concept of cloud computing services liked with the models including PaaS, IaaS and SaaS[1] which denotes everything as a service and thus cloud may assumed to have a generalized service oriented architecture. Instead of keeping data on a particular hard drive or updating applications for the current needs, a service over the internet can be used ,which is at some other location for storing information and data. Thus cloud computing allows individuals and organizations to use data and services that are managed by third parties at some remote locations. The deployment models [1] of cloud can be used categorization of service or data delivery. Some known cloud computing services include Amazon, Google, Yahoo and Salesforce.com [2].

Usually there will be Cloud Service Provider (CSP) which provides data to consumers or end-users. In the case of cloud, information's can be accessed at anywhere at any time and it generally involves remote data storage and processing. But this will involves a paradigm shift in providing services and data. This can lead to various accountability issues in the cloud computing scenario which could be major reason for loss of privacy. So to handle the issue of accountability some mechanisms [3] must be provided. In addition to that there will be certain security related issues which must also be rectified for the proper implementation of deployment models. Client side security is a serious issue in this aspect. There can be possibilities that a particular client which is acting as authorized one can be reason for security breaches, so in order to avoid such a possibility in this paper additional client side verification is done.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

II. NEED FOR ACCOUNTABILITY AND SECURITY

A well defined cloud based services must have to possess certain properties which include Accountability, Security, Availability, Adaptability and Scalability. If these properties are absent then surely this will become a prominent reason for disapproving cloud based services .Accountability is most important factor involved in providing data governance and protection of corporate and service data stored in cloud. Making Cloud accountable includes provision of data transparency and trackable. It is very important in the sense that the cloud deployment models generally include the following scenario as shown in figure1.The accountability reintroduces the trust relationship between various entities of cloud computing scenario and also helps to keep up the developer's authority over data in transit and in sharing. As a matter of fact both preventive and detective controls can be used in the case of security and accountability.

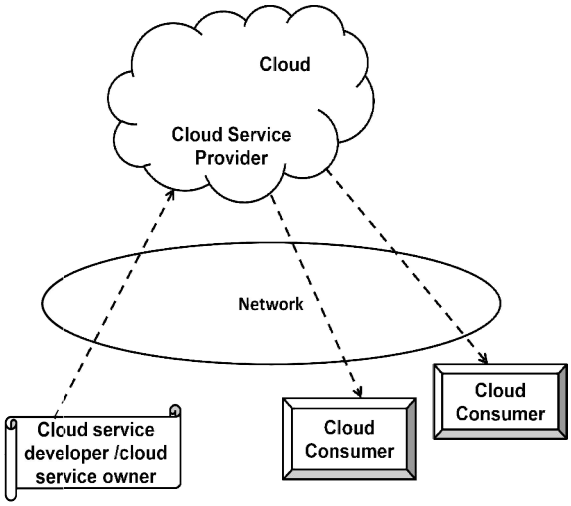

Fig 1. Cloud Computing Architecture

Security problems are mainly associated with the cloud to its highly complex nature. Especially in the case of data sharing there can be numerous problems. Cloud computing provides access to data, but Making sure that only privileged and authorised entities may access it [4] is a hurdle. Thus, cloud service providers need to build confidence with their clients by being open and accessible. It is essential to have the right safeguards in place to stop cloud service providers from utilising client data in a manner that has not been authorised [5].

Heterogeneous and much diversified services along with domains require fine grained access control policies. These access control policies should be flexible of meeting dynamic requirements in a flexible way. Also it is very important that the access control can be easily managed and well administered. In that manner the cloud service provider must be very careful in the deployment of this access privileges to prevent possible security breaches.

III. RELATED WORKS

Several solutions were proposed to obtain accountability in cloud especially for data sharing applications. In [6] an accountability It is explained how to handle end users' privacy issues before creating a privacy manager. Their fundamental premise is that users' private data is transported to the cloud in an encrypted format, where it is processed. The privacy manager[6] deobfuscates the processing's output to provide the true outcome. In this case obfuscated code will be present in cloud service provider for security reasons.

Obfuscation is term used to denote that it is a sophisticated process. Also authors used it as a main method of preventing data leakage from cloud service provider. In [7], the authors present a layered architecture for addressing the end-to-end trust management and accountability problem in federated systems. The first layer deals with authentication and authorization and second layer deals with accountability and third layer deals with anomaly detection.

A CIA [8] framework is been discussed in this for ensuring distributed accountability for data sharing in the cloud. This framework can provide both logging and auditing facilities. In addition to that here accountability can be ensured with the help of log files. This type of framework is required to provide an end to end distributed accountability which combines the access control, usage control and authentication.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

Accountability is the way of ensuring trust and transparency in the cloud environment. So this frame work can be a better option with which transparency of data usage can be maintained in the dynamic cloud environment. But in this case also security of data which is shared is not dealed yet.

IV. PROPOSED SYSTEM

The proposed system ensures distributed accountability along with secured data sharing. Here a client accountability framework is provided for data owners who actually create data and thus data's are becoming accountable with respect to each client access. Also in addition to that each and every client are required to pass through an additional key verification step before accessing any data from cloud service provider in order to increase the security of data .Usually the logging and auditing facilities also adds to the advantages of this entire framework. According to this framework access are either in the form of read or write. The chain of accountability and security with regard to this framework is as in the following figure.

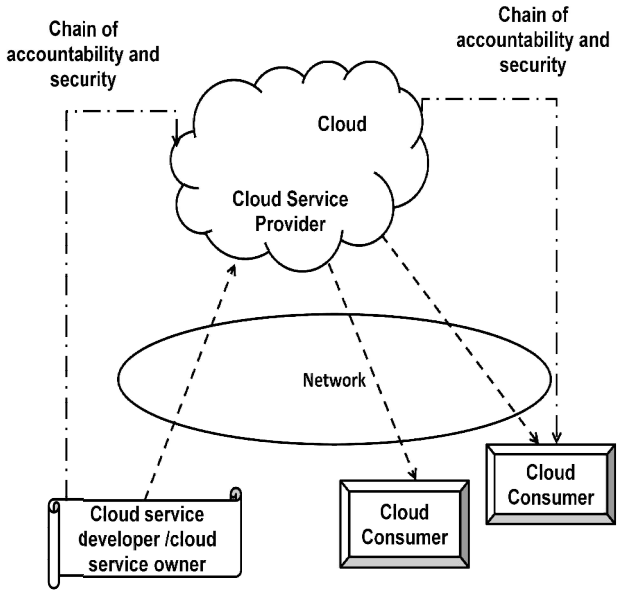

Fig 2. Security and Accountability Chain

Generally the accountability process has several steps. Initially policy planning is there to determine which details is to be logged by CSP[8] and here it will be mainly access details. As part of sensing and tracing there involves logging the expected actions in the order they are occurring in CSP. Logs are maintained as part of the next phase. The next issue is the safe keeping of logs which is absolutely important to keep log files tamperproof. The next phase is reporting the details based on log files. Auditing is generally done to check log reports for any security breaches and for highlighting loopholes. Auditing in proposed system can be push based or pull based [9].Finally based on the auditing usually problem areas are rectified and removed.

According to the proposed system in addition to accountability further client side verification is also added to improve security features as shown in Fig3. Initially the data owner creates data and associated access policies and stores it in the form of JAR files. JAR is the Java Archive File format which is a compressed file format and saves a lot of storage space. Here the Jar files have a complicated structure and it has two components, the Inner Jar and Outer JAR .Outer Jar handles authentication of entities and Inner jar is associated with encrypted files and other information to retrieve the log files. For any access from CSP the client must be authenticated and for that the client must be registered with the CSP.

For maintaining integrity of data each time a client registers to CSP it forms a file with the client information and here in this framework this information also includes a shared key given to client by the CSP. During login client has to provide this key for verification in addition to password and ID. MD5 [10] is used for this. This additional key verification can enhance security in the case of client accesses. Also data owner has to register with CSP in order to

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

store all details in CSP which is used for any accessing from CSP. Data owner stores the data in CSP in the form of JAR files and is encrypted using PBE algorithm and the password is stored for later decryption.

Each and every client access is verified with respect to the key given to at the time of registration and then only the access to CSP is provided. CSP's are also authenticated with respect certain service level agreements or by a trusted third party. For integrity purpose when client retrieval information reaches data owner, by viewing access privilege data owner verify integrity. These log files are also encrypted with PBE algorithm [11] to keep it tamperproof but using keys generated by RSA [12] during the data owner registration.

The main actions which are logged involves are as follows and this will depend on the type of access controls. This access controls determines how clients and other users are authorized to access the content from CSP.

View. In the case of view reading of data is allowed. There is no possibility for saving any raw copy of it anywhere permanently. When there is a view-only access request, the inner JAR will decrypt the data and create a temporary decrypted file. The decrypted file will then be displayed to the entity using the Java application viewer in case the file is displayed to a human user.

Download. The entity is allowed to save a raw copy of the data and the entity will have no control over this copy or neither log records regarding access to the copy. When there is a write request the download option allows the requested entity to obtain the copy of decrypted file in its own system.

Also auditing facilities are also provided .In the case of pull mode auditing usually data owner can do it when needed especially in case of emergency .In push mode for auditing a periodic update scheme is preferred. The main advantage of proposed system is there will be CSP storage availability for each data owner to store their data. Also there is separate authentication mechanism for clients with access privilege control. Only privileged clients can access data. Moreover the JAR file storage itself can avoid certain data losses.

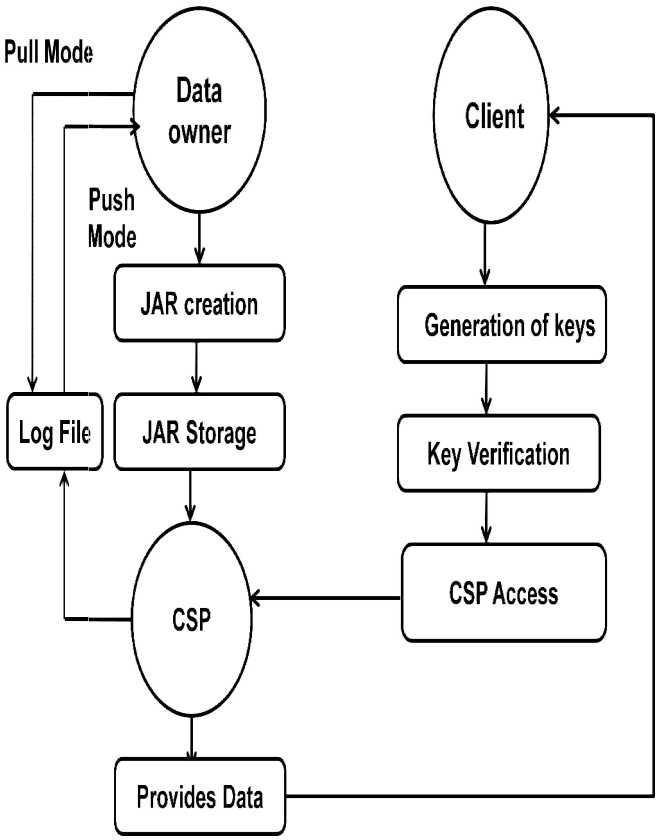

Fig.3. Framework for securing the Accountable cloud by additional Client side verification.

Also automated information service is there for data owners when data is accessed by client in order to refine integrity. Based on access privileges integrity is checked and evaluated. Also separated Logging and auditing mechanism reduces

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, August 2023

overhead. Moreover the log files should be retrievable anytime by their data owners when needed regardless of location where files are stored.

V. CONCLUSION

In this paper, privacy and security problems in the cloud are addressed which is mainly caused by data outsourcing in a different location which is different form data owner. So a fear of data loss occurs which may decrease popularity of cloud based services despite of its splendid advantages. Here an innovative approach for automatically logging any access to the data in the cloud together with an auditing mechanism is described along with added protection to stored data. This approach allows the data owner to not only audit his data but also enforce secure environment for data sharing. Moreover one of the main features of this work is that it enables the data owner to audit all the data that is being accessed. As a whole, this mechanism provides an approach for secure data sharing in the cloud which assures accountability of data by verifying integrity of data especially based on access privileges.

VI. ACKNOWLEDGMENT

The authors wish to thank the Management and Principal and Head of the Department (CSE) of Ilahia College of Engineering and Technology for their support and help in completing this work.

REFERENCES

[1]. Bhushan Lal Sahu,Rajesh Tiwari, "A Comprehensive Study on Cloud Computing"International Journal of Advanced Research in Computer Science and Software Engineering ISSN:2277 128X Volume2,Issue 9,September 2012

[2]. T. Jaeger, J. Lin, and J.M. Grimes, "Cloud Computing and Information Policy: Computing in a Policy Cloud?," J. Information Technology and Politics, vol. 5, no. 3, pp. 269-283, 2009

[3]. T. Mather, S. Kumaraswamy, and S. Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice). O' Reilly, first edition, 2009.

[4]. Takabi, Hassan ,Joshi, James B D,Ahn, Gail-Joon, "Security and Privacy Challenges in Cloud Computing Environments," Security & Privacy, IEEE,2010

[5]. A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.

[6]. S. Pearson, Y. Shen, and M. Mowbray,"A Privacy Manager for CloudComputing,"Proc.Int'l Conf. Cloud Computing pp. 90-106, 2009.

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

[8]. S. Sundareswaran, A. Squicciarini, D. Lin, and S. Huang,"Promoting Distributed Accountability in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2011.

[9]. Sundareswaran, Smitha ; Squicciarini, Anna Cinzia ; Lin, Dan "Ensuring Distributed Accountablilty for data sharing in the cloud IEEE Transactions on Dependable and Secure Computing,2012

[10]. Md. Alam Hossain, Md. Kamrul Islam, Subrata Kumar Das and Md. Asif Nashiry "cryptanalyzing of message digestalgorithms md4 and md5," International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012

[11]. Password Based Encryption http://ftp.rsasecurity.com/pub/pkcs/ ps/pkcs-5.ps

[12]. Mandeep kaur, Manish Mahajan" Using encryption Algorithms to enhance the Data Security in Cloud Computing" International Journal of Communication and Computer Technologies Volume 01 – No.12, Issue: 03 January 2013