Scientific Journal Impact Factor (SJIF): 1.711

IJMTER

International Journal of Modern Trends in Engineering and Research

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

PRIVACY PRESERVING DISTRIBUTED ACCESS TO ENCRYPTED CLOUD DATABASE

S.Mekala[1], S.Ramasami[2]

[1]PG Scholar(M.E), Angel College of Engineering and Technology, Tiruppur, India

[2]Assistant professor, Angel College of Engineering and Technology, Tiruppur, India

Abstract-Cloud computing is one of the most increasing one with the increase number of cloud users. In today's environment every user wants to access their data at any time and at anywhere. In an organization they store their data only on their computers, if they want their data during roaming situation means it is not possible one to carry the data at every time, this is a difficult factors for an organization. Cloud computing can address this problem by providing data storage mechanism to access the data at anywhere. This is one of the storage device used to access their data at any where through networks which is called cloud provider. This new concept helps to keep on tracing the real information about users and it is named as CIA . The objective center of the framework approaches the logging action for the user's data or information and also for their policies in the services. Some bars in the logging options we search for another way to get the cloud services in effective manner so we introduce the JAR (Java ARchives) capabilities in this paper. JAR helps the user or consumer to transfer the information from one place to another place. In JAR method don't have edit option for the user's data or information. The JAR programmable capability which is used to create both dynamic and traveling object. When access is made to the user data will be trigger authentication and automated logging control to JARs. A distributed auditing mechanism is used to control the users.

Keywords—Accountability, Cloud Computing, JAR file, Privacy.

I. INTRODUCTION

Today user may spend lot of time with a computer to collect lot of data over network and store it where it as portable for the user. During the roaming time user may need the data from their PC (Personal Computer) it is very difficult to take it as a portable one with large datasets. So they may problem occurred while their roaming time. For this reason storing an enough data in network can solve this problem. Cloud storage is used to avoid this problem. Cloud storage refers to storing a large amount of data which in the form of pay-per-use scheme which is referred to cloud computing. It is used to off-site storage scheme maintained by a third party i.e. cloud provider . It is most popular one to store the data in geographical environment with infinite computing resources and access the data where the user need without worry about the data loss. Hence it provides greater availability, scalability, and reliability to the users. This survey shows the features are provided by the cloud provider as a service of Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Database as a Service (DBaaS).

Cloud services

(a) Software as a Service (SaaS: This provides a service to the user by offering different software to the different user over internet. A distinct instance of service which runs in the cloud, here one or more user can utilize the service. Here no charges are detected from the user for the service or software license. In some cases charges may detected for the maintenance of the service.

(b) Platform as a Service (PaaS): This provides a service to the user for the layer of software platform. It provides a storage mechanism for the various applications and consumptions. User can have an independency to build their personal applications that provides infrastructure for the user. It offers predefined components of combined OS and the application server, e.g. LAMP platforms.

(c) Infrastructure as a Service (IaaS): This provides a service to the user for the basic storage and processor infrastructure as a service over the network. It provide a service to the computer infrastructure for the servers, network administrators, data centre, etc… to handled the workload of these service through IaaS. For this service user need to pay charges, when they use this service over network. In this mechanism cloud computing provide a service over the internet, hardware and software in datacenters as a services. The datacenter of hardware and software is called as Cloud.

(d)Database as a Service (DBaaS): This provides a service to the user for their data. It does not require modifications to the database hence it is controlled by the cloud provider. Cloud provider manage and direct the database and aim to avail the instant services to the data users. Here organizations pay for the database service for getting the service from the service provider. For the organization with fewer amounts of resources limited hardware and time-bound projects, DBaas solve this problem; it is in the bases of pay-per-usage manner. DBaaS is a successful paradigm where the data and the storage devices are located in cloud infrastructure and use the data in any where by the user.

In some case user have worry about the security and privacy problems from the cloud provider. In some cases cloud provider provide a security to the frontend resource only and failed to provide a security to the backend resources, so the attackers may hack the data easily from the backend resources. Hence malicious user could compromise the data integrity and confidentiality. Where leakage details of data might be in the users cloud resources and the cloud provider are the responsible for this issue . Thus user must provide a security from the cloud provider between the attackers and the forgoing cloud resources by encrypting their data. Encryption is a process of encoding the data in some format i.e. embedding the text in the format of ciphertext to protect data managed by untrusted server.

II. RELATED WORK

With a massive growth in user data in cloud, user requires changing data storage while their roaming, privacy and security for their personal data, better transferring data, better broadband facilities, etc... And cloud computing led to the emergence of cloud databases. For this issue this survey shows some existing techniques for solving their user problem in this review section. Ryan K L Ko et.al studied the problems and challenges of the trusted cloud, where the unauthorized user can access the entire data without disturbing the actual user. An unauthorized person may do the two things which is accessing the data and putting duplicate data because cloud storage provides a geographical database. It is not a trusted one to store the data of the users.

Ferretti, Luca, et al study two problems; which are (i) Bandwidth problem due to increase no .of database size because of encrypted data. (ii) Re-encrypted data access, the performance of re-encrypted data may take a lot of time for processing the data when it has a large number of rows. The response time for processing the data may take a lot of time to decrypt the data and the data where not a secure and also not confidential one. To solve the above issue Ferretti, Luca, et al proposed adaptive encryption mechanisms that give guarantee to the data. This mechanism is based on the Database as a Service (DBaaS) architecture for providing security to the data in cloud environment. This gives an attractive mechanism, because it does not need to define a design time. It manages the independent and distributed client application without leaking of the data.

III.CLOUD PRIVACY AND SECURITY

Cloud computing has raised a range of important privacy and security issues .Such issues are due to the fact that, in the cloud, users data and applications reside at least for a certain amount of time on the cloud cluster which is owned and maintained by third-party. Concerns arise since in the cloud it is not always clear to individuals why their personal information is requested or how it will be used or passed on to other parties. To date, little work has been done in this space, in particular with respect to accountability. Their basic idea is that the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The output of the processing is deobfuscated by the privacy manager to reveal the correct result. However, the privacy manager provides only limited features in that it does not guarantee protection once the data are being disclosed.A layered architecture for addressing the end-to-end trust management and accountability problem in federated.

IV. METHODOLOGY

Initially, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and these entities can also assign the tasks to others, etc. Second, entities are allowed to join and leave the cloud environment in a flexible manner. So, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

The algorithm here used is Log Retrieval Algorithm for Push and Pull modes. The algorithm presents logging and synchronization steps with the harmonizer in case of pure Log. First the algorithm checks whether the size of the JAR has exceeded a stipulated size or the normal time between two consecutive dumps has elapsed. The size and time threshold for a dump are specified by the data owner at the time of development of the JAR. The algorithm also determines whether the data owner has requested a dump of the log files. If none of these events has happened it proceeds to encrypt the record and write the error correction information to the harmonizer. The interaction with the harmonizer begins with a simple handshake. If no response is received the log file records an error. The data owner is then altered via emails, if the JAR is configured to send error notifications. Once the handshake is done, the interaction with the harmonizer proceeds using a TCP/IP protocol. If either of the aforementioned events has happened, JAR simply dumps the log files and resets all the variables, to make a space for a new record. In case of Access Log checks whether the CSP accessing the log satisfies all the conditions specified in the policies pertaining to it.

V. MODULE DESCRIPTION

5.1. CREATION OF DATA OWNER FILE MODULE

In this module, the data owner uploads their data in the cloud server. The new users can register with the service provider and create a new account and so they can securely upload the files and store it. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file. To allay users' concerns, it is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud.

5.2 CALCULATION OF JAR FILE MODULE

In this module we create the jar file for every file upload. The user should have the same jar file to download the file. This way the data is going to be secured. The logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. Every access to the user's data should be correctly and automatically logged.

This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed. Log files should be reliable and tamper proof to avoid illegal insertion, deletion, and modification by malicious parties. Recovery mechanisms are also desirable to restore damaged log files caused by technical problems. The proposed technique should not intrusively monitor data recipients' systems, nor it should introduce heavy communication and computation overhead, which otherwise will hinder its feasibility and adoption in practice.

5.3 CLOUD SERVICE PROVIDER

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud with the jar file created for each file for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

5.4 PRODUCTION OF JAR FILE

In this module we show how our system is secured by evaluating to possible attacks to disassemble the JAR file of the logger and then attempt to extract useful information out of it or spoil the log records in it. Given the ease of disassembling JAR files, this attack poses one of the most serious threats to our architecture. Since we cannot prevent an attacker to gain possession of the JARs, we rely on the strength of the cryptographic schemes applied to preserve the integrity and confidentiality of the logs. Once the JAR files are disassembled, the attacker is in possession of the public IBE key used for encrypting the log files, the encrypted log file itself, and the *.class files. Therefore, the attacker has to rely on learning the private key or subverting the encryption to read the log records.

To compromise the confidentiality of the log files, the attacker may try to identify which encrypted log records correspond to his actions by mounting a chosen plaintext attack to obtain some pairs of encrypted log records and plain texts. However, the adoption of the Weil Pairing algorithm ensures that the CIA framework has both chosen cipher text security and chosen plaintext security in the random oracle model. Therefore, the attacker will not be able to decrypt any data or log files in the disassembled JAR file. Even if the attacker is an authorized user, he can only access the actual content file but he is not able to decrypt any other data including the log files which are viewable only to the data owner.1 From the disassembled JAR files, the attackers are not able to directly view the access control policies either, since the original source code is not included in the JAR file. If the attacker wants to infer access control policies, the only possible way is through analyzing the log file. This is, however, very hard to accomplish since, as mentioned earlier, log records are encrypted and breaking the encryption is computationally hard. Also, the attacker cannot modify the log files extracted from a disassembled JAR. Would the attacker erase or tamper a record, the integrity checks added to each record of the log will not match at the time of verification, revealing the error. Similarly, attackers will not be able to write fake records to log files without going undetected, since they will need to sign with a valid key and the chain of hashes will not match.

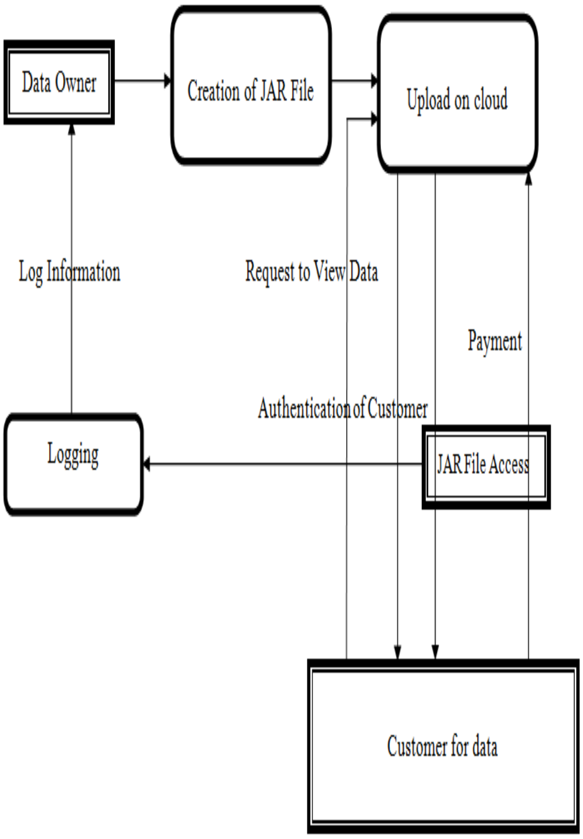

Fig 1.1 Architecture of the system

5.5 INTRUSION DETECTION MODULE

In this module, an attacker may intercept messages during the authentication of a service provider with the certificate authority, and reply the messages in order to masquerade as a legitimate service provider. There are two points in time that the attacker can replay the messages. One is after the actual service provider has completely disconnected and ended a session with the certificate authority. The other is when the actual service provider is disconnected but the session is not over, so the attacker may try to renegotiate the connection. The first type of attack will not succeed since the certificate typically has a time stamp which will become obsolete at the time point of reuse. The second type of attack will also fail since renegotiation is banned in the latest version of OpenSSL and cryptographic checks have been added.

5.6 VERIFICATION OF DATA OWNER MODULE

The cloud sever is connected to the JAR for the authentication response and request. But in the JAR file don't have the edit option so to overcome this issue, we propose the new technique called provenance controls to JAR. By using this control the data's can be read or write by the user. In this JAR, maintains the error correcting and sends the original data's to the user.

VI. CONCLUSION AND FUTURE WORKS

To preserve the user's data or information on the internet is very important. The user data's known by the unauthorized person means leads to misbehaviors. Before proposing this paper, there is no solution for this kind of misbehaviors from the third persons or unknown person. So first proposing against the improper activities is automated logging access by using the auditing mechanisms and then CIA. In CIA framework also leads to some obstacles in the data sharing service in the cloud. To overcome those problems we approach the new technique as JAR files. In the JAR programming capabilities the data sharing between the two people is carried out in effective manner. But edit options in not found in the JAR. So we implement new idea for that, we introduced the provenance controls technique in this paper. Our proposed technique works in efficient manner as showed through simulation and experimental analysis of our work.

REFERENCES

[1] Shraddha B. Toney and Sandeep U.Kadam," Cloud Information Accountability Frameworks for Data Sharing in Cloud - A Review" International Journal of Computer Trends and Technology- volume4Issue3- 2013

[2] SmithaSundareswaran, Anna C. Squicciarini and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transaction on dependable a secure computing, VOL. 9, NO. 4, pg 556-568, 2012 .

[3] Ms.P.Angaiyarkanni, and Mr.C.Ramesh "A Decentralized Data Distribution Assessment for Virtual Storage System"- International Journal of Computer Science and Management Research Vol 2 Issue 2 February 2013

[4] Hui Wang "Privacy-Preserving Data Sharing in Cloud Computing"- Journal of Computer Science and TechnologyMay 2010, Volume 25, Issue 3, pp 401-414

[5] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. EuropeanConf. Research in Computer Security (ESORICS), pp. 355-370, 2009.

[6] Marco Casassa Mont, Ilaria Matteucci, Marinella Petrocchi,MarcoLucaSbodio(marco.casassamont@hp.com,ilaria.matteucci@iit.cnr.it, marco.sbodio@gmail.com)-"Enabling Data Sharing in marinella.petrocchi@iit.cnr.it, in the cloud.

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

[8] R. Corin, S. Etalle, J.I. den Hartog, G. Lenzini, and I. Staicu, "ALogic for Auditing Accountability in Decentralized Systems,"Proc. IFIP TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.

[9]Luca Ferretti, Michele Colajanni, and Mirco Marchetti,(2014)'Distributed concurrent access to encrypted cloud database,' IEEE Trans. vol. 25, no.

[10]Armbrust, M.(2011) 'A View of Cloud Computing,' Comm. of the ACM, vol. 53, no. 4, pp. 50-58.

[11]Agrawal,D.F. and Abbadi, A.E. (2012) 'Databae Management as a Service: Challenges and Opportunities,' Proc. 25th IEEE Int'l Conf. Data Eng.