ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

SURVEY ON ACCESSING ENCRYPTED DATABASE IN CLOUD

S.Mekala[1], M.Senthil Prabhu M.E[2], V.Gayathri[3]

PG Scholar (M.E), Angel College of Engineering and Technology, Tiruppur, India [1,3]

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

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. For this service user worry about the security and privacy issue under this cloud computing for their personal data. For this issue this survey shows various techniques for the security and privacy mechanism for the user data.

Keywords: Cloud provider, Cloud Services, Distributed data, Access Control, Data Privacy and Security

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 [1]. 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:
(i) 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 [2].

(ii) 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 [2].

(iii) 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.

(iv)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 [3].

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 [3]. 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. LITERATURE REVIEW

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 [4] 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.

For this problem Ryan K L Ko et al proposed a TrustCloud framework, to achieve a trusted cloud to the user, to provide a service by making use of detective controls in cloud environment. Detecting process has the accountability access with the cloud. Here user is a responsible person for their data, hence user must tell the accountability with the technical and policy based services. By providing the accountability through user it may solve the problem from the untrusted one. Hence this approach provides privacy, security, accountability and auditability.

Muhammad Rizwan Asghar et.al [5] discusses the problems of enforcing security policies in cloud environment. With the high growth of data in cloud they where problem arises due to untrused person access of the data. To ensure the security is immature, they didn't ensure for the safe data in cloud environments. Security problem is a great issue; here we enforce the security for the owner's data. Providing high security they may high expensive for the users.

For the above mentioned problem Muhammad Rizwan Asghar et.al proposed an ESPOON policy which is Encrypted Security Policies for OutsOurced eNvironments. This policy is used to address the above problem and give better confidentiality to the users. It provides a better security by separating the security policy and the enforcement mechanism. Here M R Asghar uses an encrypted scheme to protect the user's data. This is used to protect confidentiality policies based on user's policy. This method has two main scheme, which is policy deployment and policy evaluation scheme.

Policy deployment is used to exploit the user's guidelines and the policy evaluation is used to estimate the user guidelines. By using this method user can safe their data.

L Ferretti et al [6] studied the problem of data leakage of the legitimate user in cloud environment by the cloud provider; they didn't give better security to the user for their personal data or internal data. Main problem arise because of no encrypted data were found, and also it provide the security for the frond-end database only and not controlled the backend database, so the malicious attackers may gain the data access to the outsourced data.

L Ferretti et al studied the problem and proposed a multiple key based scheme to allow the database administrator to obtain a cryptographic key for high access control policies. By providing this key scheme it based on multi user mechanism so every time a key will be generated to the actual user for the data access. By using the key, user may decipher it and use the data over cloud. It provides the service for public cloud DaaS. It enforces the access control mechanism. By this enforcement user can guaranteeing in their data. It minimizes the data leakage problem.

A.J. Feldman et al [7] find the issues of leaking data in server side and study the risk of privacy problem. Due to centralization of information attackers may easily hack the data through cloud computing. Access control under this cloud provider is not a strong one; user data may loss at any time because all a user is not always in the online to check the status of the data. So it is easy to hack the data in anytime by the attackers and also they may modify their data at any time so it is risky one.

For addressing this issue A.J. Feldman et al proposed a SPORC, for the untrusted server. It study only the encrypted data, it cannot terminate the mechanism until correct execution were done. It is generated in web based applications for privacy guarantees to the user. Their goal is to store the data in encrypted format in both the cloud and the local copy of the shared condition. This SPORC system synchronized the data for provide privacy to the users. It collaborate the word processing and instant message with an untrusted server. And it also contains the detecting mechanism to find out the hackers and their process by using operational transformation and fork* consistency protocols.

Ferretti, Luca, et al [8] 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. It is based on the aware mechanisms soothe user can guaranteed their data confidentiality and allow the cloud provider to over take a large set of data over encrypted data.

III. CLOUD COMPUTING SECURITY THREATS AND SOLUTION

Distributed Data: - This mechanism is used to share the data of the user in networks while their roaming when the user need. Data distributed among different locations, need concurrent access of an encrypted data. To preserve data privacy and stability of the user data; we have to eliminate the intermediary server between the user and the cloud provider. Among different providers may taking advantage of secret sharing. Without intermediate server data distribution can done in secure level [1].

Privacy issues: - A Privacy issue is one of the main issues for the data user who stored their data in the cloud environments [2]. Every user may want their personal data in private manner. Sometimes cloud provider compromise the data to the malicious attackers, so the problem may occur for the data user. With the use of external provider data may loss, so user must make sure who is accessing the data and who is maintaining the server at every time to protect their data. For this privacy issues user can encrypt the data so no one can access the data.

Encryption is one of the best methods to protect the data. Encryption is based on embedding the text into some format it may be ciphertext, audio embedding process.

Control issues: - Controlling the data from the unauthorized is one of the main issues for outsourced data in a cloud. Physical control is one of the best methods for the control mechanism and at the same time every time physical control is not a possible one from the unauthorized one [9, 10]. When compare to physical scheme an automatic control mechanism can provide a secure one in the possible of every time. Visualization is one of the important one to control the users data and maintain control over access to user resources. This control mechanism is ability to control the deployed applications and potentially application of the user.

Concurrent and independent access: - Concurrently and independently access in a cloud in important one for a cloud database service, protecting data privacy to the user data by allowing a cloud database to perform concurrent operations over an encrypted data, for eliminating a trusted broker or trusted proxy [11]. For this concurrency and independent model Secure Database as a Service (SDBaaS) integrate cloud database with secure provider manner for data Privacy and security. Concurrency model is used to Read/Write operation with the user database in a secure manner [12].

Identity and Access management: - In cloud computing data is stored in distributed location with a many clienta and run in extraction process with large amount of data of client information. To accessing the data over network may occur an untrustful problem because of increasing no. of attackers in networks, so who anyone can access our data without our permission which is called hacking process. To control the unauthorized access we provide a mechanism called access control tool, to control the data over distributed networks [13, 14]. Access control works in the bases of authenticate the authorized user with a sigh on mechanisms. It provides a data access matrix to monitor the accessing data limits. Here we provide a mechanism to access the data in limited manner which is controlled by the data user. Identity mechanism is used to find the unauthorized one by sign on of instant user when an actual user is signed in. this mechanism is used to manage the multiple user in a network.

IV. OUTCOMES OF SURVEY

- We have studied and analyze the problem of privacy and security issues from the cloud provider.
- Most of the researchers who where concentrate only on privacy of data transfer only but failed to concentrate on security issues of cloud provider.
- Every data users must want their data, to be a secure one in cloud environment so only they can access the data at any time and at any where through network.
- User data must not be interfered by the cloud provider or unauthorized for better data integrity.
- Confidentiality of the user private data must be secured and the access of data must be restricted to a cloud provider.
- Data must be available to the authorized user at any time for accessing data by the user without any interrupts, this is called data availability.
- User must maintain the back up of data for any future use.
- User can share their data only to the trusted one, so only security will arise.
- User or cloud provider must keep a log of Users who access data, time of event and event description; by using this we can catch the untrusted one.
- Regular auditing should be conducted by the user to monitor the activity.
- Encryption /decryption key should be kept secured by the user.
- Providers should verify the authenticity of their clients.
- Frequent data backup policy should be in place for a user security.

V. CONCLUSION

In this survey we present threats and solution of security and privacy for the cloud user. Cloud computing is one of the important for the cloud user to access the data through network at any where, so they were worried about the security problem of their personal data. Their personal data are maintained by the cloud provider. Providing security to their data is most important one for the user from the provider. Sometime user may afraid from the provider also because they may leak the data by compromise with the untrusted one. This survey studied various researchers' approaches and their drawbacks. This survey shows the security threats and their solution by analyzing and evaluating the process of data distribution, access control and privacy of user data. Hence access of encrypted data provide a secure and privacy for the user data.

VI. REFERENCES

[1] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Distributed, concurrent, and independent access to encrypted cloud databases." (2014): 1-1.

[2] ashalatha, r., and m. Vaidehi. "The significance of data security in cloud: a survey on challenges and solutions on data security".

[3] Arora, Indu, and Anu Gupta. "Cloud Databases: A Paradigm Shift in Databases." *International J. of Computer Science Issues* 9.4 (2012): 77-83.

[4] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg , Qianhui Liang , Bu Sung Lee, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" 2011 IEEE World Congress on Services.

[5] Muhammad Rizwan Asghar, Mihaela Ion, Bruno Crispo, "ESPOON Enforcing Encrypted Security Policies in Outsourced Environment", 2011 Sixth International Conference on Availability, Reliability and Security.

[6] Luca Ferretti, Michele Colajanni, and Mirco Marchetti, "Access control enforcement on query-aware encrypted cloud databases" IEEE 2013.

[7] A.J. Feldman, W.P. Zeller, M.J. Freedman, and E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources," Proc. Ninth USENIX Conf. Operating Systems Design and Implementation, Oct. 2010.

[8] Ferretti, Luca, et al. "Security and confidentiality solutions for public cloud database services." *SECURWARE 2013, The Seventh International Conference on Emerging Security Information, Systems and Technologies*. 2013.

[9] Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Access control enforcement on query-aware encrypted cloud databases." *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*. Vol. 2. IEEE, 2013.

[10 Ferretti, Luca, Michele Colajanni, and Mirco Marchetti. "Supporting security and consistency for clouddatabase." *Cyberspace Safety and Security*. Springer Berlin Heidelberg, 2012. 179-193.

[11] Dr. M. Newlin Rajkumar, Brighty Batley C, Dr.V.Venkatesakumar, Ancy George, Scholar, P. G., and P. G. Scholar. "Survey on the Concurrency Control Protocols for Encrypted Cloud Databases."

[12] S.M. Hema Latha , S.Ganesh, "A Brief Survey on Encryption Schemes in Cloud Environments"-2013.

[13] Pathak, Ajeet Ram, and B. Padmavathi. "Survey of Confidentiality and Integrity in Outsourced Databases."

[14] Khan, Abdul Wahid, et al. "A Literature Survey on Data Privacy/Protection Issues and Challenges in Cloud Computing." *IOSR Journal of Computer Engineering (IOSRJCE) ISSN* (2012): 2278-0661.