International Journal of Advanced Research in IT and Engineering

ISSN: 2278-6244

OPTIMAL STORAGE SERVICES IN CLOUD COMPUTING ENSURING SECURITY

Yathi Raja Kumar Gottapu*

A. Raja Gopal**

Abstract: *Cloud computing is a technology which uses internet and remote servers to stored data and application. Cloud computing provides on demand services. Multiple users want to do business with their data using cloud but they get fear of losing their data. While data owner store his/her data on cloud, he must get confirmation that his/her data is safe on cloud. To solve above problem in this paper we provide effective mechanism to track usage of data using accountability. Accountability is checking of authorization policies and it is important for transparent data access. We provide automatic logging mechanisms using JAR programming* which *improves security and privacy of data in cloud. Using this mechanism data owner may know his/her data is handled as per his requirement or service level agreement.*

Keywords: *Cloud computing, accountability, security*

*Department of Computer science and Engineering, Lakireddy Balireddy College of Engineering, Mylavaram

**Assistant Professor, Department of Computer science and Engineering, Lakireddy Balireddy College of Engineering, Mylavaram

I. INTRODUCTION

A cloud normally contains virtualized computing resources, which could be allocated to the different purposes within short time periods. The whole process of requesting and receiving resources is typically automated and is completed in minutes. The cloud computing is the set of software, hardware, networks, storage, services and interfaces that combines to deliver aspects of the cloud computing as a service, share resources, software and information are provided to computers and other devices on demand. It allows people to do things they want to do on a computer without the need to buy and build an IT infrastructure or resources, to understand the underlying technology.

Through cloud computing clients can access standardized IT resources to deploy new applications, services or computing resources quickly without reengineering their entire infrastructure, hence making it dynamic. The core concept of cloud computing is reducing the processing burden on the users terminal by constantly improving the handling ability of the cloud. All of this is available through a simple internet connection using a standard browser.

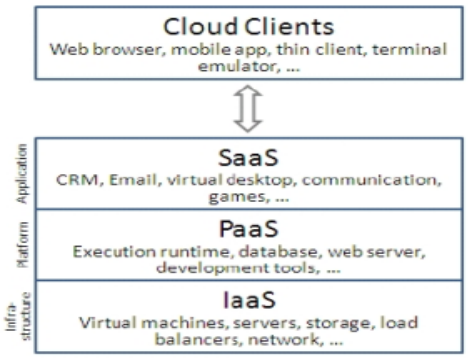

Fig: cloud computing layers

From the viewpoint of data security, which always been an important part of quality of service Cloud computing certainly positions a new challenging security fears for number of reasons. Firstly, customary cryptographic primitives for the purpose of data security protection cannot be directly agreed due to useless control of data under Cloud Computing. Therefore, certification of correct data storage in the cloud must be directed without definite knowledge of the whole data. Bearing in mind various kinds of data for each user stored in the cloud and the demand of long term continuous declaration of their data safety, the problem of authenticating correctness of data stored in the cloud becomes

even more challenging. Secondly, Cloud Computing may not be reliable because of third party data warehouse. The data stored in the cloud may be recurrently modified by the users, including insertion, modification, appending, deletion, reordering, etc.

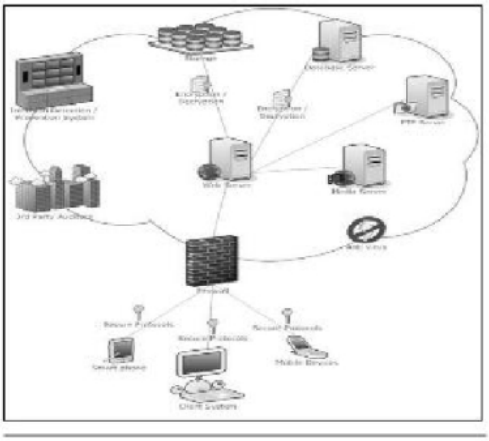

Fig: Cloud storage architecture

To ensure storage correctness under dynamic data update has the utmost importance. On the other hand, this dynamic feature also makes traditional integrity insurance techniques ineffective and demands new solutions. Last but not the least, the organization of Cloud Computing is powered by data centers running in a synchronized, cooperated and distributed manner. Individual user's data is stored redundantly in multiple physical locations to reduce the data integrity threats.

Accountability is likely to become a fundamental concept in cloud that grows the trust in cloud computing. It helps to secure the user's data, shielding sensitive and trusted information, improving user's trust in cloud computing.

II. LITERATURE SURVEY

In this section review related works had done addressing security in cloud. Security issues are very important in cloud. There are many techniques available. S. Pearson et al describe privacy manager mechanism, in which user's data is safe on cloud. In this technique the user's data is in encrypted form in cloud and evaluation is done on encrypted data. The privacy manager makes readable data from result of evaluation manager to get the correct result. In obfuscation, data is not present on service provider's machine so there is no risk with data, so data is safe on cloud. But this solution is not suitable for all cloud applications, when input data is large, this method can still require a large amount of memory [2]. In [3], the authors present procedural and technical solution both are

producing solution to accountability for solving security risk in cloud in this mechanism these policies are decided by the parties who use, store or share that data irrespective of the jurisdiction in which information is processed. But it has limitations that data processed on cloud is in unencrypted while processing so there is a risk of data leakage. In [4], the author gives a language which permits to serve data with policies by agent. Agent should prove their authorization to use particular data. In this logic data owner has to attach Policies with data, which contain a description of, which actions are allowed with which data. But there is the problem of Continuous auditing of agent, but it cannot prevent modern threats. The actions should be monitored and agent should give justification for their action. After that authority will check the justification. In [5], authors give a three layer architecture which protects information leakage from cloud. It provides three layers to protect data, in first layer the service provider should not view confidential data. In second layer service provider should not do the indexing of data. In third layer user specify use of his data and indexing in policies, so policies always travel with data. In [6], authors present accountability in federated system to achieve trust management. The trust towards use of resources is accomplished through accountability. So to resolve problem for trust management in federated system they have given three layers architecture. First layer is authentication and authorization. The authentication is done using public key cryptography. Second layer is accountability which perform monitoring and logging. The third layer is anomaly detection which detects misuse of resources. This mechanism requires third party services to observe network resources.

III. CLOUD COMPUTING SECURITY

Cloud store the mass amount of users' data, so well- known security is very important. The vendor of the data does not aware about where their data is stored and they do not have control of where data to be placed. Here it searches the security experiments in cloud. Some of the security risks consist of secure data transfer, data separation, security of stored data, user access control, and secure software interface. To promote JAR file compression method and security concern of end users accountability mechanism are used. Here the basic concept is that user's private data should be sent to the cloud in an encrypted form and then with the encrypted data, processing is carried out.

IV. ACCOUNTABILITY FOR THE CLOUD

Accountability become a fundamental concept in cloud that helps for growth of trust in cloud computing. The term Accountability [I] refers to a contracted and accurate requirement that met by reporting and reviewing mechanisms. Accountability is the agreement, to act as an authority to protect the personal information from others. Accountability is for security and protect against use of that information beyond legal boundaries and will be held responsible for misuse of that information. Accountability uses preventive controls. Preventive controls for the cloud include risk analysis, policy enforcement, trust assessment, obfuscation techniques, decision support tools and identity management. Surveying accountability uses detective controls. Detective controls for the cloud including reporting, auditing, tracking, and monitoring. Accountability in cloud motivates, keeping the data usage trackable and transparent.

V. PROPOSED WORK

Cloud computing is a large infrastructure which provide many services to user without installation of resources on their own machine. This is, pay as you use model. Examples of the cloud services are Yahoo email, Google, Gmail and Hotmail. There are many users, businesses, and government uses cloud. So data usage in cloud is large. So data maintenance in cloud is complex. Many Artists wants to do business, of their art using cloud. For example one of the artists wants to sell his painting using cloud then he want that, his paintings must be safe on cloud and no one can misuse his paintings.

There is a need to provide technique which will audit data in cloud. On the basis of accountability, we proposed one mechanism which keeps use of data transparent means data owner should get Information about usage of his data. This mechanism support accountability in distributed environment. Data owner should not bother about his data. He may know his data is handled according to service level agreement and his data is safe on cloud. Data owner will decide the access rules and policies. User will handle data using these rules and logs of each data access have been created. In this mechanism there are two main components i.e. logger and log harmonizer.

The logger is with the data owner's data, it provides logging access to data and encrypts log record by using public key which is given by data owner and send it to log harmonizer. The log harmonizer is performing the monitoring and rectifying. It generates the master key, which holds decryption key decrypting the logs and at the client side

decryption. It sends key to client. In this mechanism data owner will create private key and public key, using generated key. Owner will create logger which is a JAR file (JAVA Archives), it includes his policies like access policies and logging policies with data send to cloud service provider.

Authentication of cloud service will be done using open SSL based certificates after authentication of cloud service provider. Data owner can be able to access data in JAR, log of each data usage will be created and encrypted using public key and it automatically send to log harmonizer. For integrity, log records are signed by entity which is using the data and log records are decrypted and access by owner. In push mode logs are automatically send to data owner and in pull mode owner can demand logs. So he can see access of his data at anytime, anywhere and he can do monitoring of his data [I].

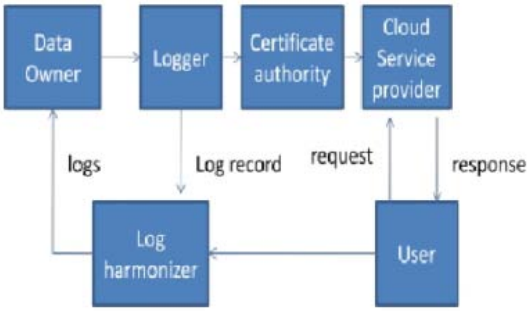

Fig : Accountability Mechanism in cloud

In Fig, working of accountability mechanism in cloud is given. When user access data then log of each access is created by logger and periodically sent to log harmonizer. Log harmonizer sends these logs to data owner. Data owner can see logs and take appropriate action if he wants. State transition diagram is, machine which shows number of states. Machine takes input from outside world and each input can produce machine to go next step. Following transition diagram shows the different states of accountability mechanism in cloud i.e. how it changes from one state to next state.

ISSN: 2278-6244

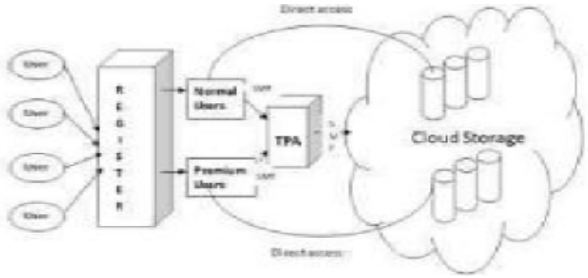

Fig: architecture of accountability trust

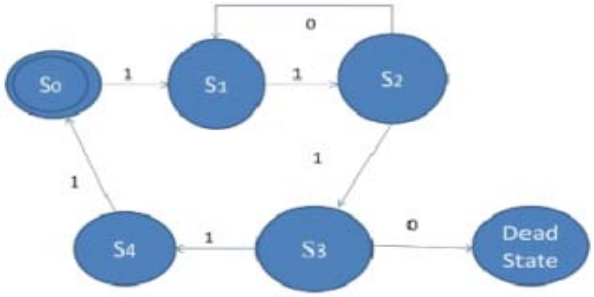

Fig: state Transition diagram

Where

0: Unsuccessful

1: Successful

Transition are:

S0 : Data Owner will send data to logger.

S1: Data Owner will create logger which is a jar file to store data and policies

S2 : Authentication of CSP to JAR file.

S3 : Authentication of user.

S4 : owner can see merge log

Input: = {0, 1} Representation of

A= ({S0, S1, S2, S3 ,S4 } {0,1}, 0, S0,δ, S4)

Input given 11011011

Expected output

δ(S0,1) = S1

δ(S1,1) = S2 δ(S2,1)= S3 δ (S3,1)= S4 δ (S4,1)= S0

In accountability mechanisms the log records are generated,

as access of data in jar happened then it create log record log rec (Lr).

Lr = r1, r2, r3,r4,…rk.

Parameters used for log record are

rk = (id, action, T, loc, h((id, action, T, loc)ri-1…..),sig)

Where,

rk = log record

id = user identification action = perform on user's data

T = Time at location loc

loc = Location

h((id, action, T, loc)ri-1...r 1) = checksum component sig= Signature of record by server

Checksum of each record is calculated and it is stored

with data. Checksum is computed using hash function

H[i] = f(H[i — I] ,m[i]), Where,

Compression function is $f = \{0,1\}^n \ X \ \{0,1\}^b$

H[i] = hash value of i^{th} log record [10],[11].

VI. CONCLUSION

This paper presents effective mechanism, which performs automatic authentication of users and create log records of each data access by the user. Data owner can audit his content on cloud and he can get the confirmation that his data is safe on the cloud. Data owner also able to know the modification of data made without his knowledge. Data owner should not worry about his data on cloud using this mechanism and data usage is transparent using this mechanism. In future we would like to develop a cloud, on which we will install JRE and JVM, to do the authentication of JAR. Try to improve security of store data and to reduce log record generation time.

VII. REFERENCES

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

[2] S. Pearson , Y. Shen, and M. Mowbray," A privacy Manager for Cloud Computing," Proc. Int'l Conf Cloud Computing (cloudcom), pp.90- 106,2009.

[3] S. Pearson and A. Charlesworth, "Accountability as a Way Forward for Privacy Protection in the Cloud, " Proc First Int'l conf. Cloud Computing, 2009.

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

[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] B. Chun and A. C. Bavier ,"Decentralized Trust Management and Accountability in Federated System," PrOC. Ann. Hawaii Int'l Conj. Sptern Science (HICSS).2004.

[7] B. Crispo and G. Ruffo, "Reasoning about Accountability within Deleption," Proc. Third Intl Conf. Information and Comm. Security (ICICS), pp.251-260, 2001.

[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] DJ. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen- barrio, J. Hendler, and 0.5. Sussman, "Information Accountability," Comm. ACM, vol. 51, no. 6, pp. 82-87,2008.

[10] B.Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons,1993.

[11] Praveen Gauravaram, John Kelesy, Lars Knudsen, and Soren Thomsen, "On Hash function using Checksums".

[12] Ryan K L Ko, Peter Jagadpramana, Miranda Mowbray, Siani Pearson, Markus Kirchberg, Qianhui, "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" HP Laboratories, pp 1 — 7, HPL-2011-38