Liability for Information sharing in Cloud

Komuravelly Sudheer Kumar, Nagendar Yamsani
Department of Computer Science and Engineering
S R Engineering College
Warangal Urban, India
sudheer_kumar_k@srecwarangal.ac.in, nagendar.y@srecwarangal.ac.in

***Abstract* - Cloud computing is a technology, which uses internet and distant servers to stored information and application. Cloud computing provides on require services. Various users desire to do trade of their information using cloud but they get panic to trailing their information. While information proprietor will store his/her information on cloud, he must get authentication that his/her information is protected on cloud. To resolve above difficulty in this paper we present helpful method to track usage of information using liability. Liability is examination of permission policies and it is important for crystal clear information access. We provide automatic classification method using JAR programming which improves safety and privacy of information in cloud. Using this method information proprietor may know his/her information is handled as per his requirement or service level agreement.**

***Keywords* -** Cloud computing, liability, safety, information sharing, privacy

I. INTRODUCTION

Cloud computing is a technology which uses internet and distant servers to store information and application. In cloud there is no need to install meticulous hardware, software on client device, so client can get the required infrastructure on his device in low-priced charge/tariff. Cloud computing is an infrastructure which provides helpful, on order group services to use various resources with a smaller amount of effort. Features of Cloud computing are, enormous admittance of information use, assets and hardware without setting up of any software, user can access the information from any device or anywhere in the world, trade can get resource in one place, that's means cloud computing provides scalability in on order services to the trade users. Everyone kept their information in cloud, as everyone kept their information in cloud so it becomes public so safety question increases towards private information. Information usage in cloud is very bulky by users and businesses, so information safety in cloud is very important issue to solve. Many users want to do business of his information through cloud, but users may not know the devices which actually process and host their information. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own information [1], [8].

Cloud provides platform as a service, infrastructure as a service and software as a service as three service models. Under the record as a service, this is having four parts which are as per mentioned below

- Encryption and Decryption - For safety purpose of information stored in cloud, encryption seems to be perfect security solution.
- Key administration - If encryption is necessary to store information in the cloud, encryption keys can't be store there, so user requires key administration.
- Authentication - For accessing stored information in cloud by certified users.
- Authorization – Privileges given to user as well as cloud provider.

To resolve the safety issues in cloud; other user can't read the individual users information without having right to use. Information proprietor should not bother about his information, and should not get fear about damage of his information by hacker; there is need of safety mechanism which will track usage of information in the cloud. liability is compulsory for monitor information handling, in this all actions of users like sending of file are cryptographically linked to the server, that performs them and server maintain secured record of all the actions of earlier period and server can use the earlier period records to know the exactness of act. It also provides dependable information about usage of information and it observes all the records, so it helps in make trust, relationship and reputation. So liability is for verification of authentication and authorization. It is powerful tool to check the authorization policies [9].liability describes permission requirement for information usage policies. Liability mechanisms, which rely on after the fact verification, are an smart way to put into effect permission policy [7].,

There are 7 phases of liability

1) Policy set with information
2) Use of information by users
3) Classification
4) Unite logs

5) Fault correctness in log
6) Audit
7) Fix and development.

These phases may change as per structure

First the information proprietor will set the policy with information and throw it to cloud service provider (CSP), information will be utilize by users and logs of each record will be formed, then log will be combined and fault correction in log has been done and in audit logs are checked and in last phase development has been done [12].

In the next figure steps of liability is given. These are 7 steps, each step is key to perform next step, liability is nothing but justification of user events means user having privileges for access this information or not. Suppose user will do mistreatment of information or resources then network or information proprietor will take action on it so users, trade and administration should not worry about their information on cloud.

II. LITERATURE SURVEY

This part addresses safety and associated workings in cloud. Safety matter is very important in cloud there are lots of techniques on hand so here is analysis of all these.

S. Pearson et al describes privacy manager method in which user's information is safe on cloud , in this technique the user's information is in encrypted structure in cloud and evaluating is made on encrypted information, the privacy manager make legible information from result of evaluation manager to get the right result. In obfuscation information is not present on Service provider's device so there is no risk with information, so information is safe on cloud, But this elucidation is not fitting for all cloud application, when input information is big this scheme can still need a large sum of memory[2]. In [3], the authors present procedural and technical solution both are producing answer to liability to solving security risk in cloud, in this mechanism these policies are determined by the parties that use, store or share that information irrespective of the authority in which information is processed. But it has restriction that information processed on SP is in unencrypted at the spot of processing so there is a risk of information outflow. In [4], the writer gives a language which permit to provide information with policies by agent; agent should attest their act and permission to use particular information. In this logic information proprietor attach Policies with information, which contain a description of which actions are permitted with which information, but there is the problem of constant auditing of agent, but they provide solution that incorrect behavior. Should monitor and agent should give justification for their action, after that authority will check the justification. In [5], writer gives a three layer design which protect information leakage from cloud, it provides three layer to protect information, in first layer the service provider should not view confidential information in second layer service provider should not do the indexing of information, in third layer user specify use of his information and indexing in policies, so policies always travel with information. In [6], authors present liability in associated system to achieve faith management. The trust towards use of assets is accomplished through liability so to resolve problem for trust management in associated system they have given three layers architecture, in first layer is authentication and authorization in this authentication does using public key cryptography. Second layer is liability which perform monitoring and logging. The third layer is anomaly discovery which discover use wrongly of assets. This method requires third party services to monitor network resources.

III. PROPOSED WORK

Cloud computing is a large infrastructure which provide many services to user without installation of resources on their own device. This is the compensate as you use model. Examples of the cloud services are Yahoo email, Google, Gmail and Hotmail. There are lots of users, trade, administration uses cloud, and so information usage in cloud is large. So information maintenance in cloud is difficult. Many performers want to do trade of their skill using cloud. For example one of the artist want to vend his work of art using cloud then he want that his work of art must be protected on cloud no one can misuse his paintings.

There is a need to provide technique which will audit information in cloud. On the basis of liability, we proposed one method which keeps use of information clear means information proprietor should get information about usage of his information. This method support liability in distributed environment. Information proprietor should not worry about his information, he may know his information is handled according to service level agreement and his information is safe on cloud. Information proprietor will decide the right to use rules and policies and user will handle information using this rule and logs of each information access have been created. In this mechanism there are two main components i.e. logger and log harmonizer.

The logger is with the information proprietor's information, it provides logging access to information and encrypts log record by using public key which is given by information proprietor and send it to log harmonizer. The log harmonizer is performing the monitoring and rectifying, it generates the master key it holds decryption key decrypting the logs, and at the client side decryption it sends key to client. In this mechanism information proprietor will create private key and public key, using generated key proprietor will create logger which is a

JAR file (JAVA Archives), it includes his policies like access policies and logging policies with information send to cloud service provider.

Authentication of cloud service provider has been done using open SSL based certificates after authentication of cloud service provider user can be able to access information in JAR, log of each information usage has been 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 information and log records are decrypted and access by proprietor. In push mode logs are automatically send to information proprietor and in pull mode proprietor can demand logs, so he can see access of his information at anytime, anywhere and he can do monitoring of his information [1].

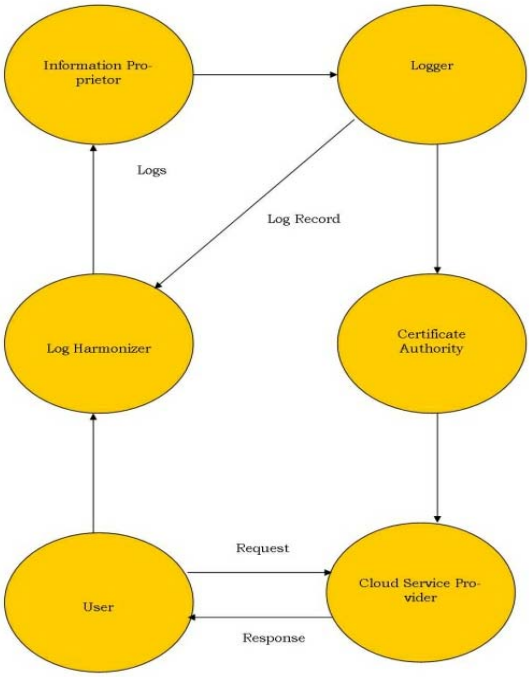

Figure 1. Liability Method in cloud

In Fig. 1 working of liability method in cloud is given. In this when user will access information then log of each contact is created by logger and periodically sent to log harmonizer, log harmonizer send these logs to information proprietor and information proprietor can see logs and take appropriate action if he wants. Following transition diagram shows the different states of liability method in cloud i.e. how it changes from one state to next state.

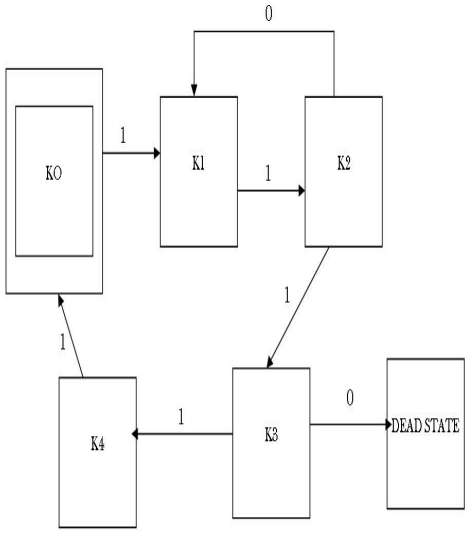

Figure 2. State Transition Diagram

Where,

0 : Unsuccessful

1 : Successful

Transition are :

K0 : Information Proprietor will send Information to logger.

K1: Information Proprietor will create logger which is a jar file to store Information and policies .

K2 : Authentication of CSP to JAR file.

K3 : Authentication of user.

K4 : Proprietor can see merge log

Input: = {0, 1}

Representation of

A= ({K0, K1, K2, K3 , K4, } {0, 1}, δ, K0 , K4 *)*

Input given 11011011

Expected output

δ(K0,1) = K1

δ(K1,1) = K2

δ(K2,1) = K3

δ(K3,1) = K4

δ(K4,1) = K0

In liability method the log records are created as access of Information in jar happened then it create log record log rec (Lr).

$$Lr = r1, r2, r3, r4... rk.$$

Parameters uses for log record are

$$rk = (id, action, T, loc, h((id, action, T, loc)ri-1…r1), sig)$$

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…r1) = 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

$$H[i] = f(H[i - 1] ,m[i]),$$

Where,

Compression function is

$$f = \{0, 1\}\ n \times \{0, 1\}b \ \ \{0,1\}n$$

H[i] = hash value of ith log record [10], [11].

IV. **CONCLUSION**

This paper presents effective method, which performs automatic verification of users and creates log records of each information contact by the user. Information proprietor can review his content on cloud, and he can get the affirmation that his information is safe on the cloud. Information proprietor also able to know the duplication of information made without his knowledge. Information proprietor should not worry about his information on cloud using this method and information usage is clear, using this method.

In future we would like to build up a cloud, on which we will mount JRE and JVM, to do the validation of JAR. Try to improve security of store information and to reduce log record generation time.

ACKNOWLEDGMENT

Authors would like to express sincere gratitude to management and principal of S R Engineering College, for their support and encouragement to carry out the research work.

REFERENCES

[1] Smitha Sundareswaran, 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.
[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 TC1 WG1.7 Workshop Formal Aspects in Security and Trust, pp. 187-201, 2005.
[5] Squicciarini , S. Sundareswaran and D. Lin, " Preventing Information Leakage from Indexing in the Cloud," Proc. IEEE Int'l Conf. Cloud Computing, 2010.
[6] Chun and A. C. Bavier ,"Decentralized Trust Management and Accountability in Federated System," Proc. Ann. Hawaii Int'l Conf. System Science (HICSS), 2004.
[7] Crispo and G. Ruffo, "Reasoning about Accountability within Delegation," Proc. Third Int'l Conf. Information and Comm. Security (ICICS), pp. 251-260, 2001.

AUTHORS PROFILE

Komuravelly Sudheer Kumar received Master's degree in Computer Science and Engineering in 2014 from Jawaharlal Nehru Technological University, Hyderabad, India. He is an Assistant Professor at the S R Engineering College, Warangal from 2010 to till date. His research areas include Cloud Computing and Information Safety.

Nagendar Yamsani received Master's degree in Computer Science and Engineering in 2009 from Jawaharlal Nehru Technological University, Hyderabad, India. He is an Assistant Professor at the S R Engineering College, Warangal from 2009 to till date. His research areas include Networks Security, Automata and Data Mining.