Ensuring Accountability for Data Sharing in Cloud

K. Rajendra Naidu[1], N.Naveen Kumar[2]

[1](*M Tech, Computer Science, School of Information Technology (SIT)/ Jawaharlal Nehru Technological University, Hyderabad, AP, India)*

[2](*Assistant Professor, Computer Science, School of Information Technology (SIT)/ Jawaharlal Nehru Technological University, Hyderabad, AP, India)*

ABSTRACT: *Cloud computing is emerging rapidly as part of latest developments in communication trends and technology. It brought revolution in today's world among key stakeholders like service providers and consumers. As a result, Leading IT industries and consumers changed the traditional way of doing business and swiftly started moving towards cloud computing technologies to lessen the burden of cost among consumers in a tailored fashion. The key challenge is how secure is the user information stored in the cloud and the mechanism to establish the information shared is to the responsible designated or authorized users as per the service agreement. To address this concern, in this paper we proposed the design with an aim of distributed accountability among key stakeholders like cloud service providers who store and manage the information, the owner who uploads the information into the cloud and the users who download the information as per the access polices. The owner will store the information in encrypted form using Advanced Encryption Standard (AES) encryption techniques, the service providers will ensure the users who register with cloud are identified and are allowed to download information if the identity is established. The cloud user is allowed to download the information once the process is followed and access controls are satisfied. For every information download request, the information will be decrypted on fly and also log will be generation in encrypted form. Owner will download the log periodically and decrypt it to get the downloaded details about the users. By periodic audits, we can ensure the information stored in the cloud is used judiciously by the responsible stakeholders as per the service level agreements.*

Keywords *– Cloud, Accountability, Security, Encryption, Data Sharing*

1. INTRODUCTION

To ensure accountability for information sharing in cloud, we first identified the stakeholders for reference in this paper as 1) Data Owner - who stores the information in cloud with cloud service provider, 2) Cloud service provider who provides cloud service and 3) Cloud user how uses cloud service provider to download information uploaded by the data owner.

Data owner develops an application to store information in cloud by availing services provided by the cloud service provider with an objective of storing information in secure way and allowing information access to only those cloud users who met the access policy. To design this, data owner first chooses cloud service provide and finalizes service level agreement (SLA) for storing information and the access policies over the information uploaded into cloud. Once service level agreement is done, owners develop an application with key features like uploading the information along with access polices for downloading information by the users. Application also designed with other features like to view the list of data files stored in the cloud, to define and edit the access polices and to view the list of cloud users who downloaded the information for auditing purpose.

The cloud service provider provides cloud service as per the SLA and will host the application and data files in the cloud. The users first register with cloud and subsequently allowed to view and download the files uploaded by the data owner as per the access polices.

The data owner prior to uploading the data files first encrypts the data files using the AES algorithms to ensure the information is secure and to restrict if from unauthorized access unless the cloud users are obliged by the access polices. The application is designed in such a way that it enables

to encrypt data files before uploading information into the cloud and also to log the cloud user details who downloaded the information in an encrypted format on fly and will store log contents in cloud and also communicates the log information to a predefined server or application owned by the data owner for accessing the log details for audit purpose. Data owner periodically use the logs and decrypt the log contents for audit purpose with the help of secret AES key. Also data owner defines and ensures the accountability for data storing and sharing in cloud among the data owner, cloud service provider and cloud users. The owner will keep the encryption key secretly without sharing to anyone. The cloud service provider will share the cloud user details who identified themselves from authentication point of view by logging it. The cloud user first establish their identity with cloud provider before access the cloud application and attempt to access the data files uploaded by the data owner. By comparing the application log details an audit mechanism is used to ensure the accountability for data storing and accessing the information from the cloud as per the SLA's and access policies defined.

2. PROBLEM STATEMENT

Data Owner wants to store files like photos or any other text file in cloud with the following requirements.

1. Data owner wants to store files in cloud such that the file contents should not be viewed by anyone including service provider.

2. Access policy will be defined such that the cloud users will be allowed to access it only if they have to identify themselves with cloud service provider first. Subsequently users are allowed to download information once the designated charges are paid prior to downloading the file.

3. Data owner wants to access log's details frequently to view the downloaded files details along with cloud user details

With the above requirements, we aim to design and develop novel approach with encryption techniques for data encryption and logging mechanism for audit.

3. CLOUD INFORMATION ACCOUNTABILITY.

In this section, we discuss about the key modules designed for the application and its purpose. The following are the three key modules for the application.

1. Data Owner Module
2. Cloud Service Provider Module
3. User Module

3.1 DATA OWNER MODULE

Data owner module is responsible to store data into cloud environment and to perform admin related activities like uploading data into cloud, viewing user profiles and managing user profiles, granting access for downloading and defining access policies, getting log details for audit trail. Data owner develop an application which will allow encryption of data files using AES algorithm that are supposed to be uploaded into the cloud. Data owner maintains the key without sharing to anyone. The key will be subsequently used on fly to decrypt the encrypted data files and also to encrypt log connects that are stored in the cloud so that it will not be changed. A mechanism will be enabled to access the logs and also the cloud users who identified themselves with cloud service provider and accessed the data owner application. By performing audit on log files, the owner identifies for any fraudulent activity involved by anyone for accessing the data files.

3.2 CLOUD SERVICE PROVIDER

Cloud service provider module is to process data owner request for storing data files and application and also provides cloud users log details to data owner for audit purpose.

3.3 USER MODULE

User module enables user registration process with the application, to manage profile details and data download request from cloud.

4. DATA FLOW DIAGRAMS

The following sections details level 0 and level 1 data flow diagrams (DFD) to depict input output and process.

4.1 DFD LEVEL 0: CONTEXT LEVEL DIAGRAM

The below diagram depicts Level 0-Context diagram for ensuring accountability for

data sharing in the cloud. It takes data and other access information from the data owner and selected Cloud Service Provider(s) for storing the information as input. User is also one of input entity which access information stored in the cloud.

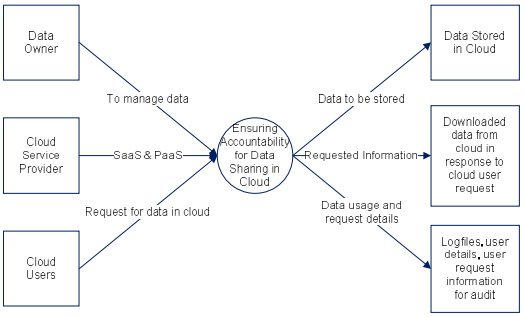

Fig 4.1: Context level diagram for ensuring accountability for data sharing in the cloud

4.2 DFD Level 1: Context Level Diagram

The below diagram depicts Level 1 process for ensuring accountability for data sharing in cloud. Main process identifies the scenario and subsequently forwards to the respective process to process the data..

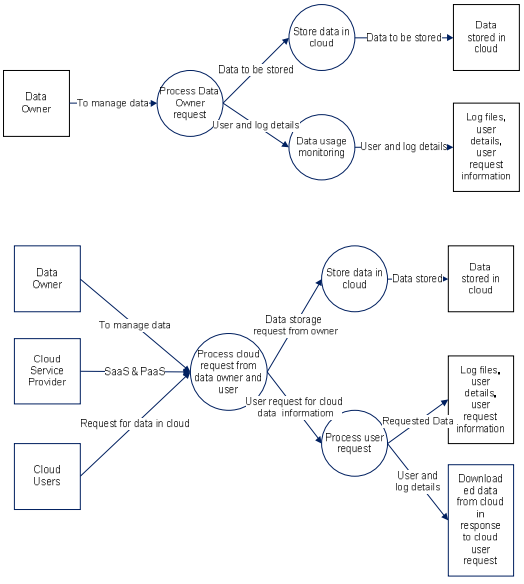

Fig 4.2: Level 1 diagram for data owner, cloud service provide and users process

I. CONCLUSION

By using AES algorithm we are able to successfully encrypt and decrypt information there by restricting from unauthorized access to the information from the cloud by cloud users. Future enhancement is to implement the application by using latest efficient encryption algorithms and also to implement third party authentication mechanism for establishing the identity of the cloud user by integrating the owner application. Integration of payment system with the owner application to process the payments needs enhancement before allowing the cloud user to access the cloud information.

REFERENCES

[1] William Stallings, Pearson Education , 4th Edition, "*Cryptography and Network Security*" text book

[2] Atul Kahate, McGrawHill, 2th Edition ,"*Cryptography and Network Security*" text book

[3] Roger S Pressman, 6th edition, McGrawHill International Edition 2005, "*Software Engineering: A practitioner's approach*"

[4] Simtha Sundareswaran, Anna C.Squicciarini *"Ensuring Distributed Accountability for Data Sharing in the Cloud"*, published in *IEEE 2012, Vol 9, No 4*

[5] P.T Jaeger, J.Lin, and J.M. Grimes,*"Cloud Computing and Information Policy: Computing in a Policy Cloud?"* J.Information Technology and Politics, *vo5, no 3,pp.269-283,2009*