Assure Security of Data in Cloud Environment

[*]Neenu Avarachan, [**]Rasheeda Z Khan

[*] Department of Computer Science and Engineering, [**]Department of Information Science and Engineering
Shreedevi Institute of Technology, Mangalore

***Abstract*-** Cloud computing is an advanced emerging technology. The cloud environment is a large open distributed system. It is important to preserve the data, as well as privacy of users. And cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. The main issue in cloud computing is the data security. So here introducing a well defined security method in cloud computing environment. To implement this technique here adopted a method that is attribute based encryption with hierarchical structure of users.

***Index Terms*-** Secure Data, Secured Deletion, Cloud Computing, Access Control, Privacy in Cloud.

I. INTRODUCTION

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing, and service oriented architecture.[1]. Cloud computing promises several attractive benefits for businesses and end users. Three of the main benefits of cloud computing includes:

- **Self-service provisioning**: End users can spin up computing resources for almost any type of workload on-demand.
- **Elasticity**: Companies can scale up as computing needs increase and then scale down again as demands decrease.
- **Pay per use**: Computing resources are measured at a granular level, allowing users to pay only for the resources and workloads they use.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction - by National Institute of Standards and Technology [8]. Cloud computing represents a real paradigm shift in the way in which systems are deployed [9].

The cloud computing Architecture of a cloud solution is the structure of the system which is shown in figure 1, which comprises on-premise and cloud resources, services, middleware, and software components[2], and the system architecture of the software system involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over a loose coupling mechanism such as a messaging queue. Although cloud computing has changed over time, it has always been divided into three broad service categories:

Infrastructure as a service (IaaS): It is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the internet.

Platform as a service (PaaS): It is a paradigm for delivering operating systems and associated services over the internet without downloads or installation.

Software as service (SaaS): Involves outsourcing the equipment used to support operations, including storage, hardware, servers and networking and networking components.

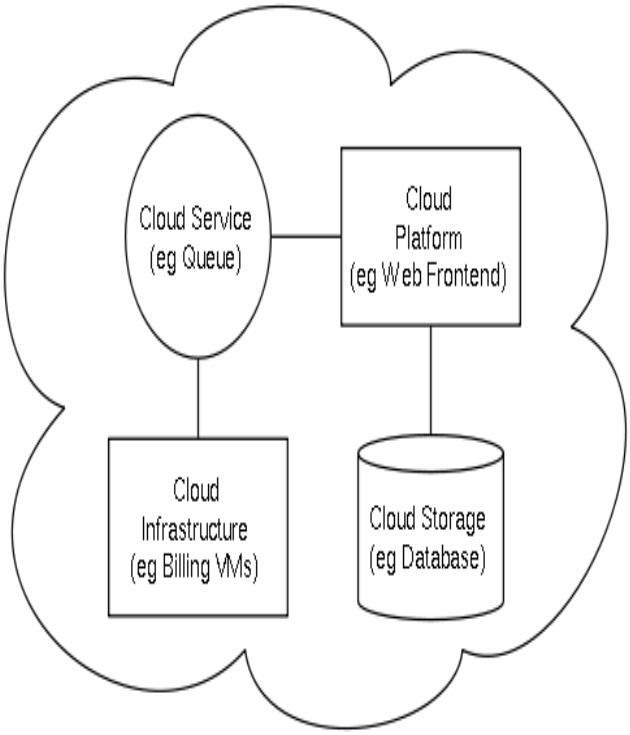

Figure 1: Cloud Architecture

There are five layers in cloud computing model, the client layer, application layer, platform layer, infrastructure layer. In order to address the security problem every layer should have security implementation [2].

Data Security is the more and more important part of the cloud environment. In the real world there are many methods for the safety of data but that methods are not providing well security. For avoiding the above problems here introducing a new mechanism for the data security in cloud.

II. RELATED WORK

In this section, I review the different existing techniques for the data security which are proposed by others. After that I am introducing about a new method for the data storage in the cloud computing.

One kind of data security is Attribute based security, which is introduced by Abdul Raouf khan[3].In this method the data security is effective only in unchangeable distributed system. The other method is introduced by Young-Gi,Hyo-Jin and Young-Hwan Bang [2]. This method [2] only told about the different kinds of attacks. The prevention method is not specified there. The next method is explained by Ynag tang and Patrick P.C[4]. This method also using Attribute based encryption method but is not acceptable in, when server and user in different domain. Then the another method is based on some Hierarchical structure[1], is introduced by Zhiguo Wan, June's Liu. Here the data is not secure because the encryption method is not flexible. Then YanZhu and his team introduced temporal access control in cloud computing [5]. In this method also the service provider and user in same trusted domain otherwise it will not work. The other method is introduced by Ming Li,Shucheng Yu and their team[6]. Here the data is keeping based on attribute based encryption but it is not applicable in multiple level. Then the next method is introduced by B.K.Onankunju [7]. In this method also the data is not secure in encryption time.

III. PROPOSED SCHEME

A. Structure of proposed model:

The proposed models have a hierarchical structure as shown in the figure 2. The hierarchical structure contain mainly three components. That is trusted authority, domain authority, and the user/owner. The trusted authority acts as the root of trust and authorizes the top level domain authorities. And this top level domain authorities authorizes the cloud users. Here consider both the owners and the users as cloud user.

B. System Model:

This is the actual model of the proposed system. In this model total two parts are there. Cloud owner/user and the untrusted cloud. The data owner can upload his file to the cloud. To make his file more secured, first the system will encrypt the original file by a data key. Then the data key is encrypted by a control key is based on a policy. The policy is assigned by the top level authority that is trusted authority. When the user sent a request to access a file, the key manager will encrypt the file based on Attribute Based Encryption (ABE) public access key

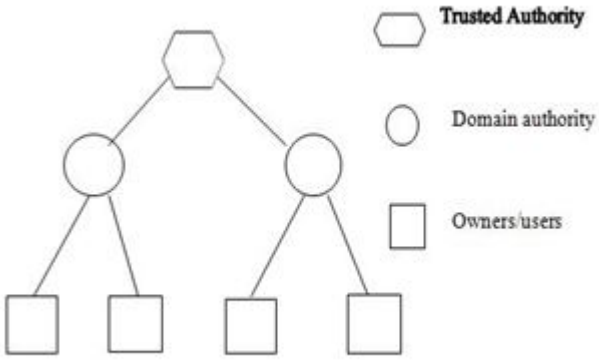

Figure 2: System Structure

and sent to the client, the client will recover the data key based on ABE private access key. The Attribute based encryption (ABE) is a scheme in which each user is identified by a policy and some function of this policy is used to determine the decryption ability for each cipher text. When the user sent a request to delete the file, the trusted authority will revoke the policy of a respective file then it's corresponding control key and data key will also remove. Then no one can access that file. Basic operations of the proposed model are,

1. Registration

To do any operation in cloud, the user and the owner should register there. For registration the user and the owner will send a registration request to the corresponding domain authority. Then the domain authority verifies that is the new member accepting there terms and conditions. If they are ready to accept the terms and conditions, then the domain authority will forward that request to the trusted domain. Then the trusted authority will provide a permanent id to each of the owners and users. Then they can set a password for them.

2. File Upload

To upload a file, first the data owner will encrypt the file using his data key and is sent to the key manager that is domain authority. Then the key manager will encrypt the data key by control key. The domain authority checks that the owner is a registered one or not. If he is a registered owner, then the domain authority will forward that encrypted file to the trusted authority.

3. File Download

To download a file the user sent a request to cloud the key manager that is domain authority. The key manager will encrypt the file by attribute based encryption- public access key with respect to the policy is assigned by trusted authority, then sent to the user. If the user satisfies that policy combination then the user can recover the data key of a file based on attribute based encryption- private access key.

4. File Deletion

To delete a file the data owner sent a request to the cloud. The domain authority first verifies the user then sent this request to trusted authority. The trusted authority revoke the policy of a respective file then the corresponding control key and the data key of a file will also remove. After that no one can access that file.

IV. CONCLUSION

In this paper, introduce the Attribute based encryption with hierarchical structure and it using a policy for the safety of data. This technique is an efficient and secure model and it is ensure the security of data in cloud environment. The main operation involved in this technique is Registration, File uploading, File Downloading and File Deletion.

REFERENCES

[1] Z.Wan, J.Liu, R.H.Deng, "HASBE:A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Forensics and Security, vol 7, no 2, APR 2012.

[2] Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and Access Control Solutions", Journel of Security Engineering, vol.2, 2012.

[3] A.R.Khan, "Access Control in Cloud Computing Environment," ARPN Journal of Engineering and Applied Sciences, vol 7, no 5, MAY 2012.

[4] Y.Tang, P.P.C.Lee, J.C.S.Lui, R.Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion," IEEE Transactions on Dependable and Secure Computing, vol 9, no 6 NOV/DEC 2012.

[5] Y.Zhu, Hu, D.Huang, S.Wang, "Towards Temporal Access Control in Cloud Computing," Arizona State University, U.S.A.

[6] M.Li, S.Yu, Y.Zheng, K.Ren, W.Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE Transactions on Parallel and Distributed Systems, vol 24, no 1, JAN 2013.

[7] B.K.Onankunju**,** "Access Control in Cloud Computing", IJSRP, vol 3, no 9, SEP 2013.

[8] P.Mell, "The NIST Definition of Cloud Computing" U.S. Department of Commerce: Special Publication 800-145

[9] B.Sosinsky, "Cloud Computing Bible", Ed. United States of America: Wiley, 2011.

AUTHORS

First Author – Ms NEENU AVARACHAN received bachelor's degree (AMIE) in Computer Science and Engineering from "The Institution of Engineers (India)" of Kolkata in 2013 and doing master's degree in Computer Network Engineering in Shreedevi Institute of technology, Karnataka.