Access Control in Cloud Computing

Bibin K Onankunju

Department of Information and Communication Technology, Manipal Institute of Technology, Mamipal, India

Abstract- Cloud computing is an advanced emerging technology. In this world the storage of data is a big headache for all. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data. The main issue in cloud computing is security. Here I am trying to introduce a new method for providing secured access control in cloud computing. This model provides a secure access control in cloud computing. To provide more secured access control it adopt a hierarchical structure and it uses a clock. Using this we can easily upload, download , delete files from and to the cloud.

Index Terms- Access Control, Cloud Computing, Privacy in Cloud.

I. INTRODUCTION

Cloud computing is one of the emerging technologies. It represents a real paradigm shift in the way in which systems are deployed [8]. As per National Institute of Standards and Technology [3], it is defined as,

"*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.*"

This cloud computing has a lot of advantages especially in ubiquitous services where everybody can access computer services through internet. With cloud computing, you can develop a device which contains a small display, processor and RAM. There is no need of other hardwares such as secondary memory. It will reduce the size of our new technology devices. Also it reduces the expences of our system.

Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software [1].The following figure shows the cloud computing model.

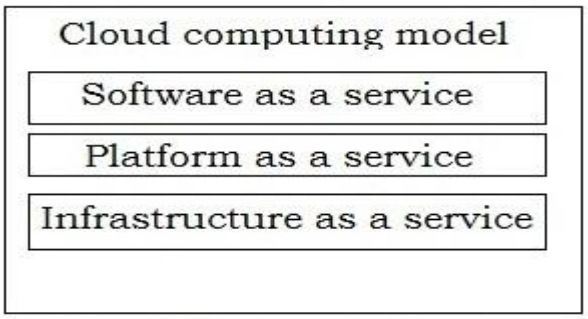

Figure 1: Cloud Computing Model

a) SaaS- To use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser.
b) PaaS- To deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (java, python, .Net)
c) IaaS- To provision processing, storage, networks, and other fundamental computing resources where theconsumer is able to deploy and run arbitrary software, which can include operating systems and applications

Along with the development of cloud applications, the cloud computing attacks are also increased. The main attacks on cloud are [1],

a) Denial of Service (DoS) attacks
b) Side Channel attacks
c) Authentication attacks
d) Man-in-Middle cryptographic attacks
e) Inside-job attacks

Due to this attacks, we need a better security policy in cloud computing. Access control is generally a policy or procedure that allows, denies or restricts access to a system [7]. It may also identify users attempting to access a system unauthorized.

Access Control allows one application to trust the identity of another application [8].The traditional model for access control is application-centric access control [1], where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures. Because in this method we need a lot of memory for storing the user details such as username and password. So cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information.

The main types of access control models are,

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)

Now we have a lot of techniques for access control in cloud computing. But these are not secured and efficient. Due to this problem, we are try to propose a new secured and efficient method for access control in cloud computing.

II. RELATED WORK

In this section, we review the different existing techniques for access control which are proposed by others. After that we will explain our proposed technique for access control in cloud computing.

One of the other main method for access control is FADE which is introduced by Y.Tang and team [5]. The method in [5] provides fine-grained access control and assured deletion for outsourced data on the cloud. But this scheme is not effectively applicable . If the data owners and service providers are in the same domain, then only it act as an effective scheme. One of the other scheme for access control is HASBE which is introduced by Z.Wan, J.Liu and R.H.Deng [2]. The main drawback of the scheme in [2] is that it is not flexible compared to other schemes.

In [10], S.Yu and team introduce a method for access control in cloud computing. In this method [10], they using KP-ABE (Key Policy Attribute Based Encryption) and PRE(Proxy Re-Encryption) . Due to the overhead of encryption and decryption, this method is not scalable.

Y.Zhu and team in [6] introduce a method for temporal access in cloud computing. In [6] these schemes are only applicable to systems in which data owners and the service providers are within the same trusted domain. The other main scheme is explained in [4] ,which is introduced by M.Li and his group . But it is very costly scheme.

In an International Joint Conference of IEEE TransCom-11, M.Zhou and his colleagues introduce a method for privacy-preserved access control for cloud computing [9]. This method [9] also has some drawbacks. But here, in this scheme, lack of flexibility and scalability make it as ineffective.

III. PROPOSED SCHEME

A. *Structure of our proposed model.*

Our proposed model have a hierarchical structure as shown in the figure 2.

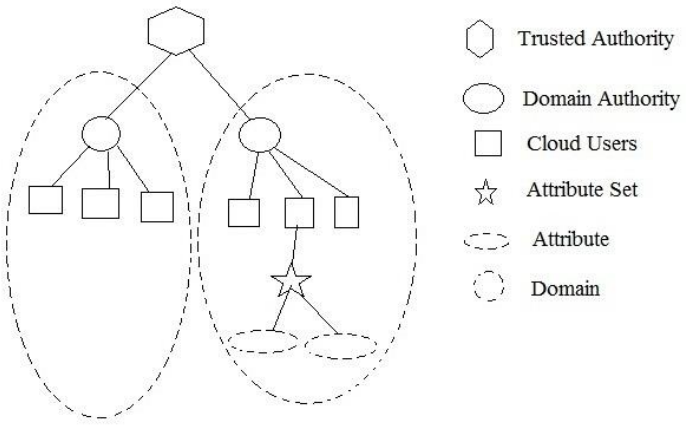

Figure 2 : System Structure

In this hierarchical structure, the trusted authority act as the root of trust and authorizes the top level domain authorities. And this top level domain authorities authorizes the cloud users. Here we consider both the owners and the users as cloud user. For each cloud users, our system keeps an attribute set which contains a set of attributes corresponding to each user. It may vary with the user. A domain contains many number of cloud users and a single domain authority. Also we use a clock to generate the key with time.

B. *System Model.*

The actual model of our system is shown in the figure 3. In this model total four parts are there. Cloud owner, untrusted cloud, clock and cloud user.

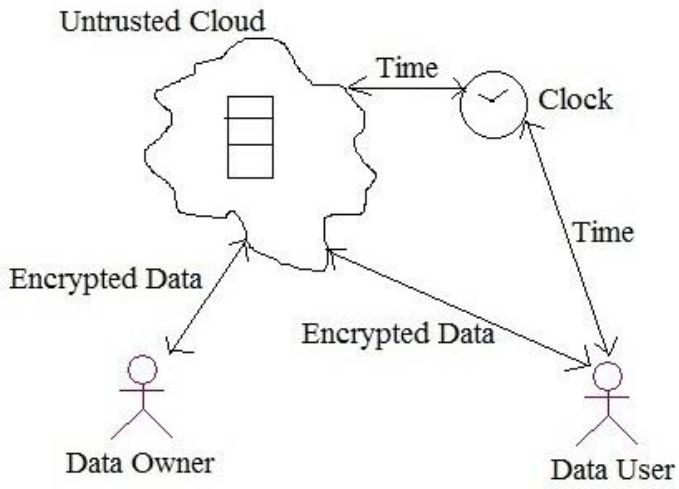

Figure 3 : System Model

Here the data owner can upload his file to the cloud. To make his file as more secured, firstly he will encrypt that file and then upload to the untrusted cloud. Only the data owner knows that the key to decrypt the files. So the uploaded files are safe in the untrusted cloud. When a data user wants to access any file from the cloud, then it send a request to the cloud. Then the cloud will forward that request to the owner. Then the owner will check the attribute set of that user. If the user have a valid attribute set, then the owner send a key to the user. When the owner send a key to the user then the clock will start counting. After a certain time period, that key becomes an invalid one. So the user should access the requested file within that time limit.

C. Basic operations of the proposed model

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 private key and send it to the next higher level. That is domain authority. Then the domain authority will 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 any file from the cloud, firstly the data user send a request to his corresponding domain authority. Then the domain authority will verify the user. If it is a valid user, then it will forward that request to the trusted authority. Then the trusted authority will forward this request to the corresponding data owner. Then the owner will check the attribute set of that user. If the user have a valid attribute set, then the owner send a key to the user. When the owner send a key to the user then the clock will start counting. After a certain time period, that key becomes an invalid one. So the user should access the requested file within that time limit.

4. File Deletion

Only the data owner can delete his file from the cloud. During the registration time of the data owner, the trusted authority will provide an id number to each of the data owners. These id numbers are permanent for them. Also each of them have a password, which is not permanent. To delete a file, the data owner firstly send a request to his corresponding domain authority. This request contains the owner id and the file name. Then the domain authority will ask password to the owner. If the owner gives the correct password, then the domain authority will forward the deletion request to the trusted authority. After that the trusted authority will delete the file from cloud.

IV. CONCLUSION

It is a highly efficient model for provide access control in cloud computing. It is in a hierarchical structure and it using a clock for providing decryption key based on time. This model ensure both security and access control in cloud computing. The main operations in this model are registration, file upload, file download and file deletion.

REFERENCES

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

[2] 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.

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

[4] 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.

[5] 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.

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

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

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

[9] M.Zhou, Y.Mu, W.Susilo, M.H.Au, "Privacy-Preserved Access Control for Cloud Computing," IEEE International Joint Conference, 2011

[10] S.Yu, C.Wang, K.Ren, W.Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," Journel from Illinois Institute of Technology.

AUTHORS

First Author – Mr Bibin K Onankunju received bachelor's degree (AMIE) in Computer Science and Engineering from "The Institution of Engineers (India)" of Kolkata in 2012 and doing master's degree in Network Engineerring in Manipal Institute of Technology, Manipal University, Karnataka.