DUAL ACCESS CONTROL FOR CLOUD-BASED DATA STORAGE AND SHARING

[1] SADA MEGHANA
[2] Mr. Naga Srinivasa Rao

[1]PG STUDENT ,DEPT OF MCA

[2] **Asst. Prof**, Dept of MCA

SREE KONASEEMA BHANOJI RAMARS P.G. COLLEGE (AMALAPURAM)

ABSTRACT

Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.

I. INTRODUCTION

One of the emerging developments is distributed computing. It addresses afundamental shift in perspective in the way frameworks are communicated [8]. "Distributed computing is a model for enabling pervasive, advantageous, on- request network access to a common pool of configurable figuring assets (e.g., networks, servers, capacity, applications, and administrations) that can be quickly provisioned and delivered with insignificant administration exertion or specialist organisation connection,"

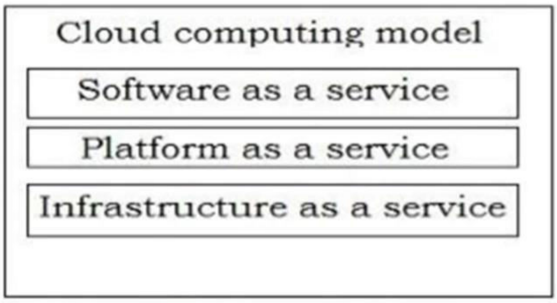


Fig 1: Cloud Computing Model

a) SaaS- To use the supplier's cloud-based apps, which are accessible from a variety of client devices via a simple client interface, such as a Web application.

b) PaaS- To upload customer-made apps to the cloud using the provider's supported programming languages and tools (java,python, .Net)

c) IaaS- To set up handling, capacity, organisations, and other basic figuring assets where the customer can deliver and run irregular programming, such as functional frameworks and applications.

Distributed computing attacks have grown in tandem with the advent of cloud applications. [1], [2], and [3] are the primary assaults on clouds.

a) Denial of Service (DoS) assaults

b) Side Channel assaults

c) Authentication assaults

d) Man-in-Middle cryptographic assaults

e) Inside-work assaults

As a result of these attacks, we urgently require a more advanced distributed computing security policy. Access control is a strategy or approach that allows,denies, or restricts access to a framework [7]. It may also detect clients attempting to gain access to an unapproved system.

One application can relay on another's identification thanks to access control [8]. The traditional model for access control, application-driven access control [1] is a comman access control architecture in each application monitors and manages its own set of clients, isn't possible in cloud-based systems. Because we need a lot of memory for this strategy, we'll need a lot of RAM to store the client's nuances, such as username and secret phrase. As a result, the cloud necessitates a client-driven access controlsystem, in which each client solicitation to any specialist organisation is packed with the client's personality and privilege data.

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control are the three basic types of access control models (RBAC)

In distributed computing, we currently have a plethora of processes for access control. These, on the other hand, are not obtained and effective. As a result of this problem, we are attempting to suggest a new and more effective access controltechnique for distributed computing.

II. RELATED WORK

In this section, we examine the various existing access control strategies proposed by others. After that, we'll explain our proposed solution for distributedcomputing access control. FADE, which was given by Y.Tang and colleagues [5], is another key approach for access control. For re-appropriated information on the cloud, the technique in [5] provides fine- grained admission control and guaranteed erasure. However, this strategy isn't actually necessary. If the information owners and specialised cooperatives are in the same area, it is a good idea. HASBE [2], a plan presented by Z.Wan, J.Liu, and R.H.Deng, is another access control plan. The main disadvantage of [2] is that, in comparison to other schemes, it is not adaptable. S.Yu and colleagues offer a distributed computing access control mechanism in [10]. They use KPABE (Key Policy Attribute Based Encryption) and PRE (Proxy Re-Encryption) in this technique [10]. This method isn't adaptable due to the increasing complexity of encryption and decoding. In [6, Y.Zhu and colleagues offer a transitory access approach for distributed computing. These approaches are only applicable in [6] to frameworks in which data owners and specialised co-ops are in the same confided in space. The other major plot is explained in [4], which is provided by M.Li and his group. It is, however, an expensive plan.M.Zhou and his colleagues describe a solution for privacy-preserving access control for distributed computing in an IEEE TransCom-11 International Joint Conference [9]. This technique [9] has a few drawbacks as well. Regardless, the lack of adaptation and versatility in this method renders it ineffective.

III. PROPOSED SCHEME

A. The development of our proposed model. As seen in Figure 2, our proposed model has a progressive construction.

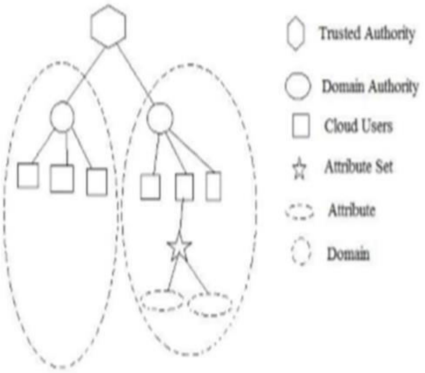


Fig 2: System Structure

The believed power serves as the foundation of confidence in this progressive structure, approving high-level space professionals. Furthermore, the cloud clients are approved by this high- level area specialist. As a cloud client, we consider both the proprietors and the clients. Our system retains a trait set for each cloud client, which contains a number of traits specific to that client. It is possible that it will change depending on the client. A space consists of a single area authority and a large number of cloud clients. We also use a clock to time the creation of the key.

A. Framework Model.

Figure 3 depicts the real-world model ofour approach. There are four sections in total in this model. Owner of the cloud, untrustworthy cloud, clock, and cloud client

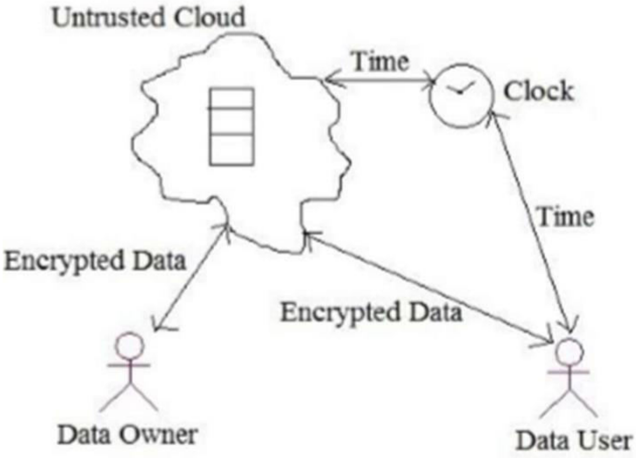


Fig 3: System Model

The owner of the data can upload it to the cloud from here. To make his record as untrustworthy as possible, he will scramble the document straight away and then move it to the untrusted cloud. Onlythe owner of the information is aware of how to decrypt the records. As a result, the transferred data is safe in the untrustworthy cloud. When an information client needs to access a record from the cloud, it sends a request to the cloud. Following that, the cloud will forward the request to the proprietor. The owner will then check the client's distinctive arrangement. If the client has a largenumber of traits, the owner will transmit a key to the client. The clock will start counting when the proprietor sends the client a key. That key becomes invalid when a certain amount of time has passed. As a result, the client must complete the requested paper within the specified timeframe.

B. Fundamental tasks of the proposed model

1. Registration

The client and the owner must both enrol in order to perform any action in the cloud. The client and the proprietor will send an enlistment request to the comparing space authority for enrollment. The space authority then confirms that the new part is complying with the agreements. If they are willing to accept the terms, the area authority will forward the request to the confided in space. The thought power will then provide everyone of the proprietors and clients with an exceptionally long- lasting id. Then they'll be able to create a secret key for them.

2. Document Upload

To convey a document to a higher level, the information owner must first encrypt it with his confidential key and then send it to the next higher level. That is the jurisdictional authority. The space authorities will then verify whether or not the proprietor is registered. If he is a registered proprietor, the space authority will send that encoded record to the confided in authority.

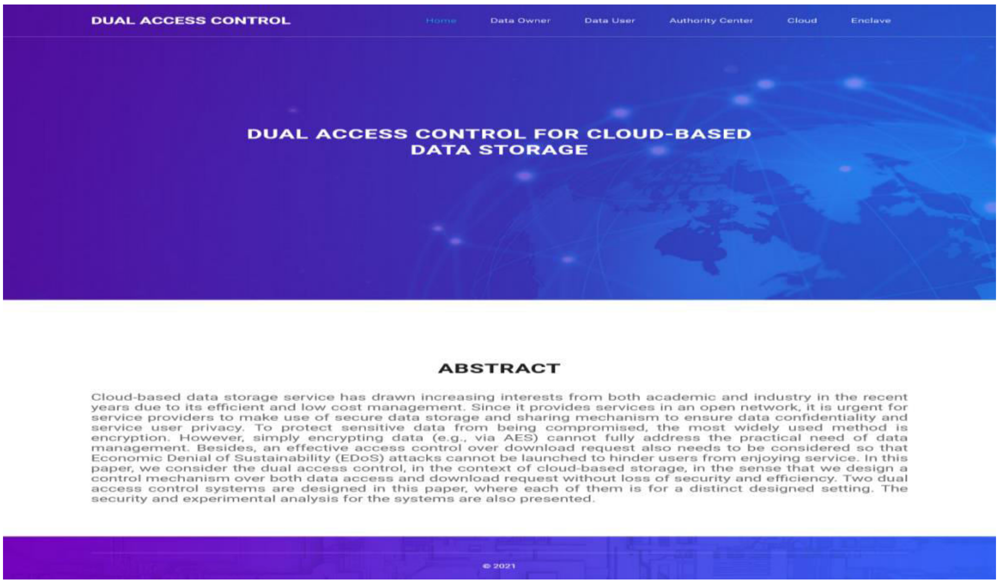
3. Document Download

To download any record from the cloud,the information client must first send a request to his corresponding space authority. The client will then be checkedby the local authority. If the client is legitimate, the request will be forwarded to the trusted in power. The believed power will then forward this request to the owner of the relevant data. The proprietor will then examine the client's trait set. If the client has a large number of traits, the owner will transmit a key to the client. The clock will start counting whenever the proprietor sends a key to a client. That key becomes invalid when a certain amount of time has passed. As a result, the client must complete the requested paper within the specified time frame.

4. Document Deletion

Only the owner of the data has the ability to delete it from the cloud. During the information proprietor's enlisting season, the believed power will assign each information proprietor an id number. Forthem, these id numbers are exceptionally long-lasting. Similarly, each of them has a secret key that isn't particularly long-lasting. To delete a document, the information owner must first file a request to his corresponding space authority. The proprietor id and document name are included in this solicitation. The area administration will then inquire about the proprietor's secret word. The area authority will forward the deletion request to the confided in power if the proprietor offers the correct secret word. The believed power will then delete the document from the cloud.

IV Results



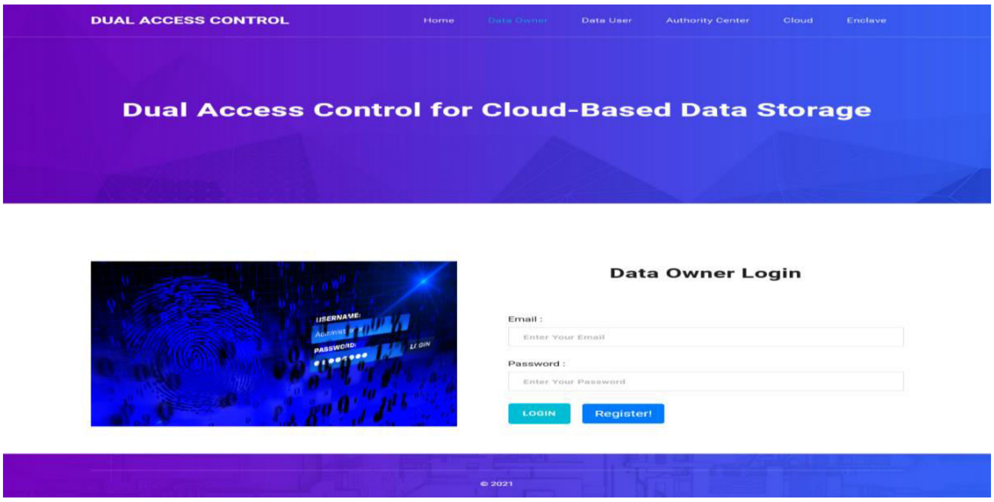
DUAL ACCESS CONTROL FOR CLOUD-BASED DATA STORAGE

ABSTRACT

Cloud-based data storage service has drawn increasing interests from both academic and industry in the recent years due to its efficient and low cost management. Since it provides services in an open network, it is urgent for service providers to make use of secure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data from being compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully address the practical need of data management. Besides, an effective access control over download request also needs to be considered so that Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, we consider the dual access control, in the context of cloud-based storage, in the sense that we design a control mechanism over both data access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper, where each of them is for a distinct designed setting. The security and experimental analysis for the systems are also presented.

© 2021

Fig 4:- home page



Dual Access Control for Cloud-Based Data Storage

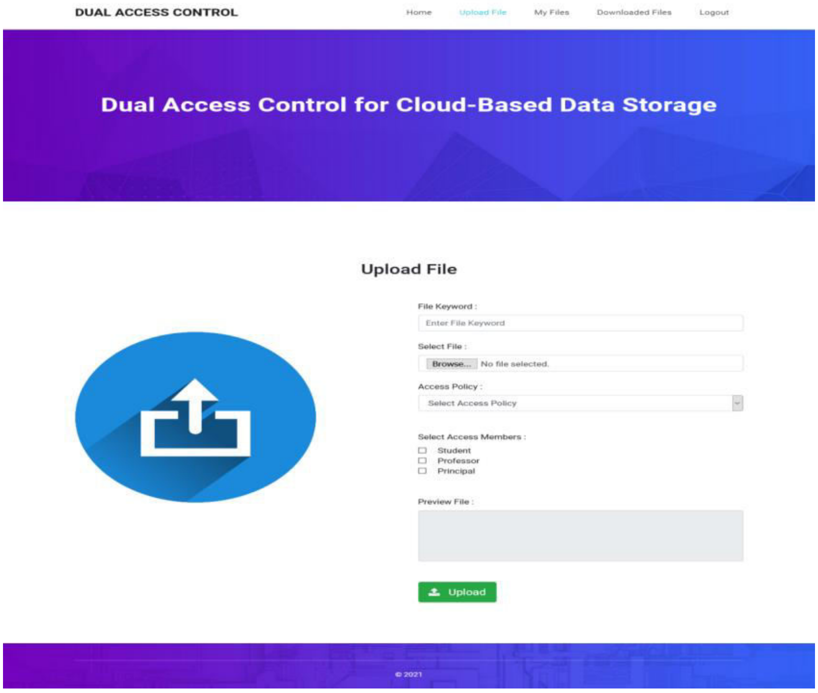
Data Owner Login

Email : Enter Your Email

Password : Enter Your Password

© 2021

Fig 5:- owner login



Dual Access Control for Cloud-Based Data Storage

Upload File

File Keyword :
Enter File Keyword

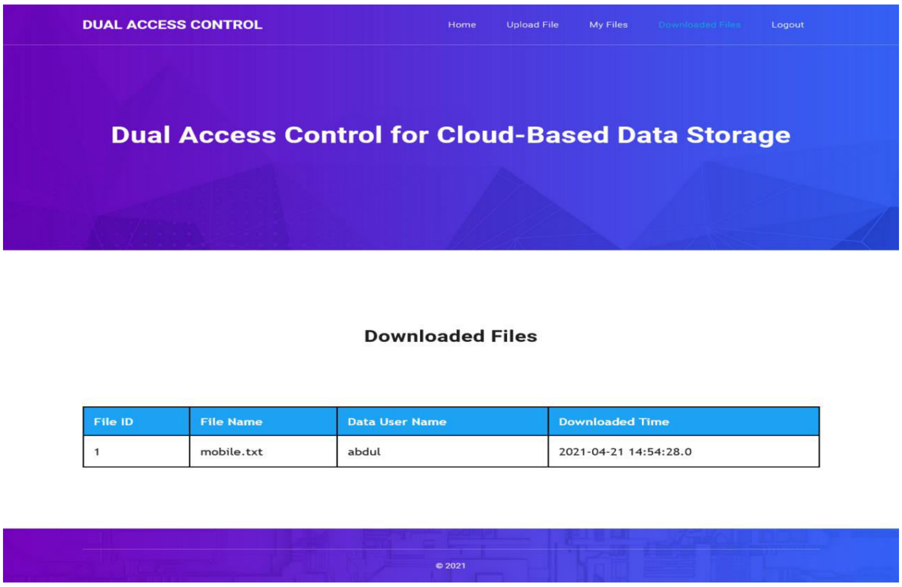
Select File :
Browse... No file selected.

Access Policy :
Select Access Policy

Select Access Members :
□ Student
□ Professor
□ Principal

Preview File :

Fig 6:- upload file

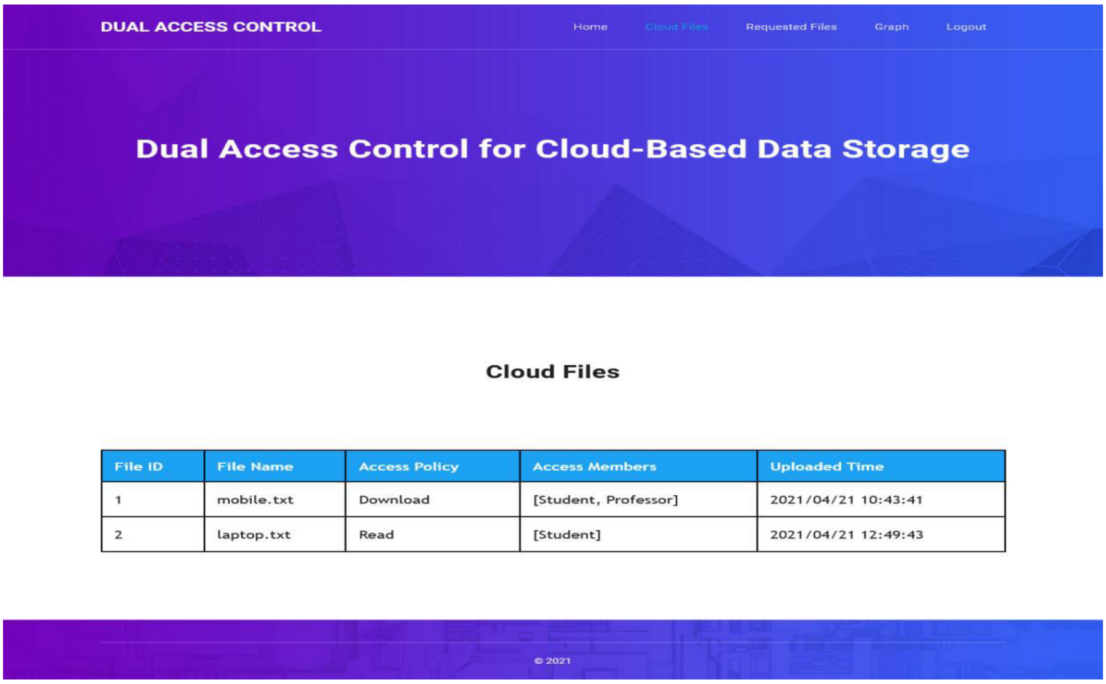


Dual Access Control for Cloud-Based Data Storage

Downloaded Files

File ID	File Name	Data User Name	Downloaded Time
1	mobile.txt	abdul	2021-04-21 14:54:28.0

Fig 6:- download file

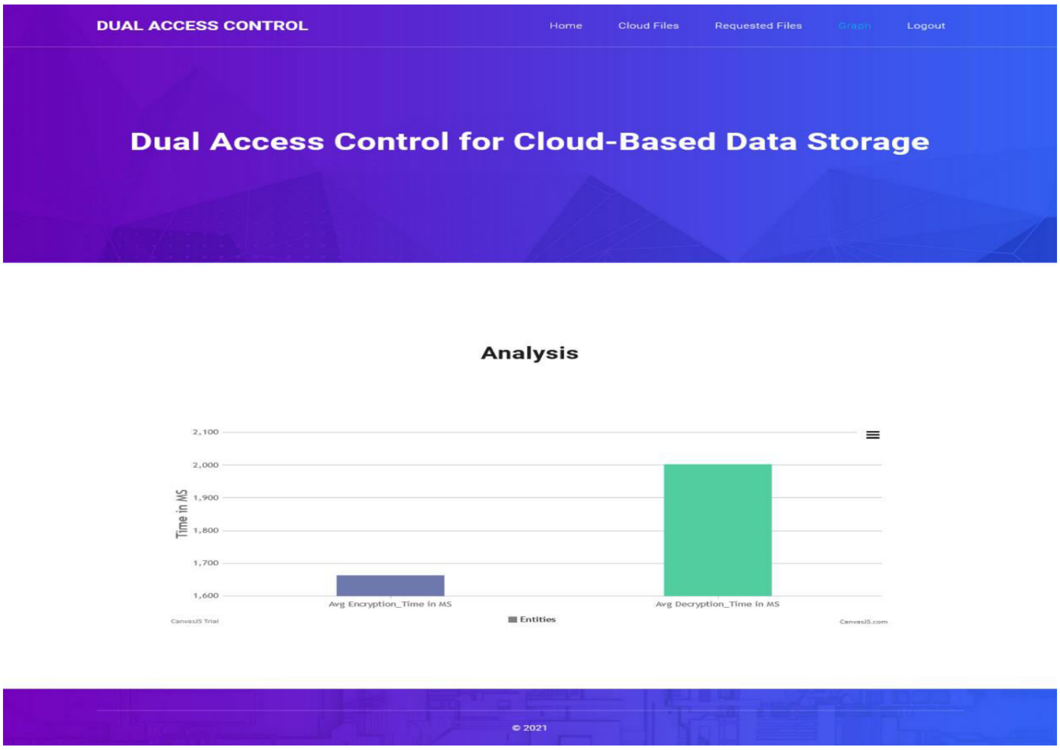


Dual Access Control for Cloud-Based Data Storage

Cloud Files

File ID	File Name	Access Policy	Access Members	Uploaded Time
1	mobile.txt	Download	[Student, Professor]	2021/04/21 10:43:41
2	laptop.txt	Read	[Student]	2021/04/21 12:49:43

Fig 7:- cloud files



Dual Access Control for Cloud-Based Data Storage

Analysis

Fig 9:- Analysis of cloud files graph

VII CONCLUSION

It is a highly efficient model for providing cloud computing access control. It has ahierarchical structure and uses a clock toprovide a time-based decryption key. In cloud computing, this paradigm ensures both security and access control. Registration, file upload, file download, and file deletion are the major operationsin this model.

VIII REFERENCES

[1] Y.G.Min, Y.H.Bang, "Cloud Computing Security Issues and AccessControl 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 Technology Transactions on Parallel and DistributedSystems, 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 CloudComputing Environment," ARPN Journalof Engineering and Applied Sciences, vol7, 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 Finegrained Data Access Control in Cloud Computing," Journel from Illinois Institute of Tech.