International Journal of Engineering Research and General Science Volume 3, Issue 4, Part-2, July-August, 2015
ISSN 2091-2730

Implementation of Role Based Access Control on Encrypted Data in Hybrid Cloud

Gajanan Ganorkar, Prof. A.B. Deshmukh, Prof M.D.Tambhakhe

Information Technology Email:g.ganorkar7691@gmail.com Contact: 8600200142

Abstract— As we know that cloud technology provides the way for storing the data.Nowdays cloud system is used for storing the large amount of user data. But there is issue of security of data in cloud storage that how we control and prevent unauthorized access to users data which is stored in cloud. To overcome this situation there is one well known access control model which is Role Based Access Control (RBAC), this model provides flexible controls and management by having two mapping, User to Role and Role to Privileges on data. This is the well known model which can be used for protecting the data in the cloud storage. Although this Role Based Access model can be used for storing the data securely in cloud system which is uploaded by the owner of data ,but this model assume that there is there is existence of trusted administrator who is going to manage all the user and role of organization which is not actually happen in real condition. In this paper we are have implemented the Role Based Encryption (RBE) scheme which can be implemented with the RBAC model for storing data securely in the cloud system. In this system user of any role who has been added by the admin of organization will have to remind only his decryption key which will be given by the admin to user when user will be added to the particular role. Based on this we have build up the hybrid cloud storage architecture which is consist of both public and private cloud, in which data will be able to store data in public cloud and organization secure data will be store on the private cloud. Access to the private cloud will be provided to only administrator of organization. Also the size of the cipher text remains constant regardless of the no. of user's in the particular role. User having higher role will be able to access the data of low level role's data. Depending on the different condition different report will be generated

Keywords— Encryption, Decryption, Public Cloud, Private Cloud, RBAC Policy, RBE Scheme, Security

.

I. INTRODUCTION

With increase in the large amount of data that need to be stored, cloud storage has attracted much attention in recent times because of its ability to deliver resource for storage to user on demand in cost effective manner. There are different infrastructures associated with the cloud [4]. One of this is a public cloud which is available to any user and user who want to use it can use in pay-as-you-go manner. Whereas private cloud is an internal cloud which is built and operated by the single organization, potentially there could be several benefits of storing data to public cloud [5]. Only organization has full access over the private cloud and private cloud cannot be accessed by the external parties. And hence we can say that private cloud is more secure than that of the public cloud.

In this research paper we have addressed the issue of storing the data on public cloud securely. Public cloud is formed by two or more data centered which are distributed geographically at different location. User does not know that where the actual data is stored and there is a strong perception that user have lost control over the data after it is uploaded to the cloud. In order to provide the control to the user for their data which is stored in the public cloud some suitable access control and mechanism is required. And this policies must restrict data access to only those user intended by the owner of data.

In this research paper we have implemented the secure RBAC (Role Based Access Control) based cloud system where access control policies will be enforced by the new Role Based Encryption (RBE) scheme. This RBE scheme enforces RBAC policies on encrypted data stored in the cloud. In this RBE scheme [13] owner of the data will encrypt the data and this encrypted data will be access by only that user which have appropriate role specified by the RBAC policy. If the user who want to access the data which is in encrypted form, if he satisfies the particular role then and only then he will be able to decrypt the data and he will be provided decryption key after satisfying the particular role. After getting the decryption key he will be able to decrypt the data and will be able to see the original content of the file that owner has uploaded to the public cloud. As shown in Fig1. We can see that public cloud is accessible to any user because data canters of public cloud can be located anywhere hence user will never know where his data is stored. In contrast to this private cloud is accessible to only administrator of the organization, Thus from this discussion we can conclude that hybrid cloud is best where shared information can be stored into public cloud and secure information can stored on the private cloud.

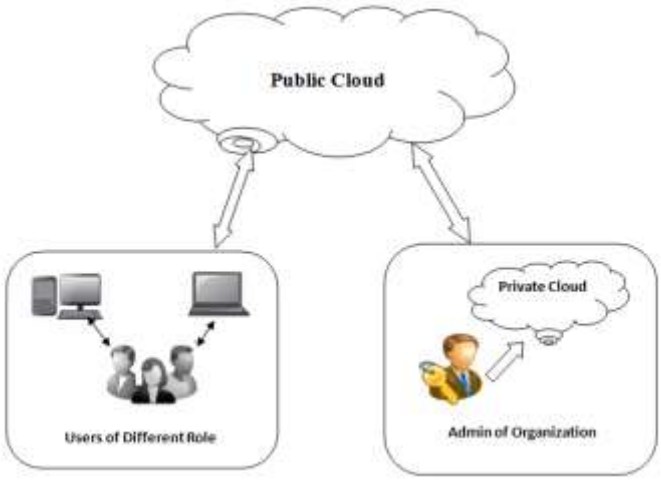

Fig1. Hybrid Cloud

In traditional access control systems, enforcement is carried out by trusted parties which are usually the service providers. In a public cloud, as data can be stored in distributed data centers, there may not be a single central authority which controls all the data centers. Furthermore the administrators of the cloud provider themselves would be able to access the data if it is stored in plain format. To protect the privacy of the data, data owners employ cryptographic techniques to encrypt the data in such a way that only users who are allowed to access the data as specified by the access policies will be able to do so. We refer to this approach as a policy based encrypted data access. The authorized users who satisfy the access policies will be able to decrypt the data using their private key, and no one else will be able to reveal the data content. Therefore, the problem of managing access to data stored in the cloud is transformed into the problem of management of keys which in turn is determined by the access policies. In this paper, we present the design of a secure RBAC based cloud storage system where the access control policies are enforced by a new role-based encryption (RBE) that we proposed in the paper.

This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation using broadcast encryption mechanism described in [5]. In proposed RBE scheme, the owner of the data encrypts the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The role grants permissions to users who qualify the role and can also revoke the permissions from existing users of the role. The cloud provider (who stores the data) will not be able to see the content of the data if the provider is not given the appropriate role. Proposed RBE [12] scheme is able to deal with role hierarchies, whereby roles inherit permissions form other roles. A user is able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner does not need to re-encrypt the data. A user can be revoked at any time in which case, the revoked user will not have access to any future encrypted data for this role. With our new RBE scheme [12], revocation of a user from arole does not affect other users and roles in the system. In addition, we outsource part of the decryption computation in the scheme to the cloud, in which only public parameters are involved.

By using this approach, our RBE scheme achieves an efficient decryption on the client side. We have also used the same strategy of outsourcing to improve the efficiency of the management of user to role memberships, involving only public parameters. Based on the proposed RBE scheme, we have developed a secure cloud data storage architecture using a hybrid cloud infrastructure. This hybrid cloud architecture is a composite of private cloud and public cloud, where the private cloud is used to storeonly the organization's sensitive structure information such as the role hierarchy and user membership information. The high level architecture of the hybrid cloud storage system is illustrated in Fig1.

In this architecture, the users who wish to share or access the data only interact with the public cloud; there is no access for public users to access the private cloud, which greatly reduces the attack surface for the private cloud. We have developed a secure cloud storage system using the new RBE scheme and hybrid cloud architecture. The most frequently used system operations such as encryption of data by a data owner, decryption of data by a cloud user have been benchmarked. The result shows that the encryption and decryption time for a given data size is constant regardless of the number of roles and users that have the access to the cloud.

II. LITERATURES REVIEW & RELATED WORK

There exist many hierarchy access control scheme [2], [6] ,[10] Which have been constructed based on hierarchical key management (HKM) schemes and approaches using HKM schemes to enforce RBAC policies for data storage are discussed in [1], [9] ,[6]. But this scheme has disadvantages that when the user's access permission is revoked, all the keys known to this user as well as all the public values related to these keys need to be changed. In the traditional control access system, enforcement is carried out by trusted parties which are usually service provider. As we know in public cloud data can be distributed at different data centre. Furthermore when owner of data upload any data to cloud the service provider itself was able to access that particular document.This raised to security issue of the document. To protect the data, data owner uses the cryptographic encryption scheme to encrypt the data in such a way that user who has decryption key was able to decrypt the data and see the original content of the data. But this scheme leads to the problem of management of keys.To overcome the drawback of above system; there is Role Based Access Control (RBAC) model which can be used to protect data which is stored in the cloud.

Although cryptographic RBAC scheme have been developed recently to secure data outsourcing, but these scheme assumes the existence of trusted administrator managing all the users and roles, which is not realistic in large-scale system. In this project work we proposed Role Based Encryption (RBE) scheme [4] which can be used efficiently with RBAC scheme to provide security to data which is stored in the cloud storage. However the revocation of user in this scheme require the update of the all the role related parameter. Another scheme was proposed [11] in this scheme the size of the cipher text increases linear with the number of all the ancestor roles. In addition if user belongs to different roles, multiple key need to be posses by this user. Moreover, the management of the user membership for each individual role requires the use of the system secret keys.

Motivation

There exist as RBAC policy i.e. User to role and role to data mapping .In RABC policy different role are created and different user are added to the role .User are added to the role according to their position and qualification in the organization. But in previous system organization has to fully trust on the service provider that they will provide security to the data of organization which may lead to the insecurity of data in cloud.Organnization doesn't know that where there data is actually stored .They simply fill that they lost control over the data which is uploaded by them.They has to fully trust on the cloud service provider.

Objectives

As we know that if we simply upload the document to the cloud the owner of the data doesn't know where actually his data is saved .The cloud provider itself is able to see the original content of the file which may lead to data access in illegal way. To overcome this situation we have implemented RBAC policy in hybrid cloud. In which all the secure information will be stored on the private cloud and public related information will be available on the public cloud. By storing their sensitive data to private cloud user knows that where the data is actually is stored .He doesn't have to worry about where his data is stored .We have implemented RBAC policy and has given permission to user to access data according to his position and qualification.

Need

1. For storing the secure data in cloud.
2. For successfully implementation of RBAC policy.
3. To overcome the problem of management of keys.

III. SYSTEM ANALYSIS

A. Exiting System

Existing system refers to the system that is being followed till now. Presently all the functionalities that can be carried out in the RBAC policy are done only by the cloud service provider. That any organization want to implement RBAC policy they has to fully trust on the cloud provider that they will provide security to the organization data. But this may lead to insecurity of data service provider may itself see the original content of data. In this existing system security was handled only by the cloud service provider and organization has to fully trust on them which may lead to sometimes insecurity of the data. Some of the main disadvantage is time consuming are as follows:

Limitatations of Existing System.

- Lack of security of data
- Organization has to fully trust on the service provider.
- Service provider itself was able to see the content of file.
- Document was uploaded to the sever in plaintext format

To avoid all these limitations and make the system working more accurately it needs to be computerized using proper database functionality.

B. Proposed System

For designing this system some modern technology is used to expose the functionality of, which is based on the Service Oriented Architecture. The technology which is used cloud Technology Integration and Interoperability of RBAC policy with Hybrid cloud, systems will contribute to more effective and efficient. Hybrid cloud is a cloud computing environment which uses a mix of on-premises, private cloud and public cloud services with orchestration between the two platforms. By allowing workloads to move between private and public clouds as computing needs and costs change, hybrid cloud gives businesses greater flexibility and more data deployment option [3].

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. Data centers of public cloud are located are at different centres even the user who uses the public cloud service don't know where his data is actually stored in opposite side private cloud is organization cloud user of private cloud know that where the actual data is store they don't have to bother about the security of the data.

In this research paper we have addressed the issue of storing the data on public cloud securely. Public cloud is formed by two or more data centres which are distributed geographically at different location. User does not know that where the actual data is stored and there is a strong perception that user have lost control over the data after it is uploaded to the cloud. In order to provide the control to the user for their data which is stored in the public cloud some suitable access control and mechanism is required. And this policies must restrict data access to only those user intended by the owner of data.

In this research paper we have proposed the secure RBAC based cloud system where access control policies will be enforced by the new Role Based Encryption (RBE) scheme. This RBE scheme enforces RBAC policies on encrypted data stored in the cloud. In this RBE scheme owner of the data will encrypt the data and this encrypted data will be access by only that user which have appropriate role specified by the RBAC policy. If the user who want to access the data which is in encrypted form, if he satisfies the particular role then and only then he will be able to decrypt the data and he will be provided the decryption key after satisfying the particular role. After getting the decryption key he will be able to decrypt the data and will be able to see the original content of the data that owner has uploaded to the public cloud.

As we know that in previous system there was some disadvantage of the traditional system i.e. to overcome this situation we have proposed the RBE scheme which can be efficiently used with RBAC scheme. To implement this project we are going to implement the hybrid cloud. This RBE scheme will contain the following four parameter.

- System administrator who has authority to generate the key for the user.
- RM is a role manager who manages the user membership of the role.
- Owners are the parties who wish to store the data securely over the cloud.
- Users are the parties who want to access the data and decrypt data stored on the cloud by the owner of the data.

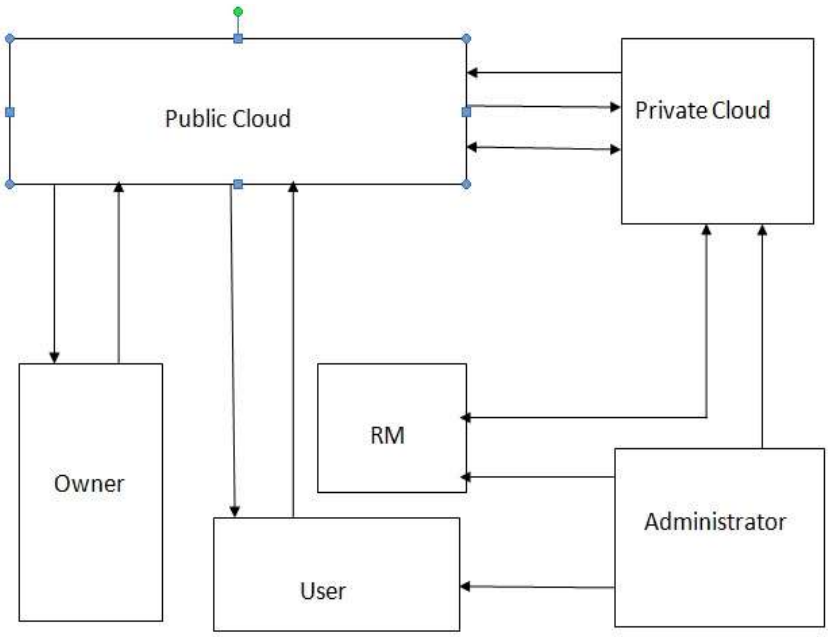

Fig2. System Architecture

As shown in above Fig2. Our system architecture is as follows the role of each component is as follows.

Owner:

Owners are the user of organization or they may be external parties who want to encrypt the data to the cloud and want is should be access by the other user. When owner of data will upload data to the cloud he will specify to whom this data should be accessed i.e. he will select the role based on the organization role hierarchy and will select the role to whom this data should be accessed.

Public Cloud:

We know that the public cloud is untrusted, because data centres of public cloud is located at different location we even don't know where our data is actually stored. Data stored in the public cloud could be accessed by unauthorized parties, such as employees of the cloud provider and users from other organizations who are also using services from the same cloud. An untrusted public cloud may deny a user's request for accessing stored data in the cloud or provide users within correct data. Such behaviours will result in the users not being able to access the data stored in cloud, but will not cause violation of RBAC policies.

Private Cloud:

As we know that private cloud is secure than public cloud because private cloud is a organizations cloud ,organization know that where the data is stored they don't have to worry about where there data is actually stored they already know it this was not possible in case of public cloud. In our project we are going to store all the security related data to the private cloud.

User:

User is the party who wish to access the data from the cloud which is uploaded by owner of data. Each user is authenticated by the administrator of the role-based system; upon successful authentication, the user is given a secret key which is associated with the identity of the user. User has not directly access to the private cloud they have only access to the public cloud.

Role Manager:

Role manager will add different role and will generate id related to the role .After this role manager will send this data to the private cloud. This role related data will be access by administrator of organization .Only role manager and administrator of organization will have direct access to the private cloud.

Administrator:

System administrator will add different user to different role which are generated by the Role Manager. He will be able to remove the particular user from the particular role. He will generate user decryption key and will send it to user via email or text message. Only Role Manager and Administrator have direct access to the private cloud.

IV. IMPLEMENTATION OF SYSTEM

In this research paper we address the issue of storing the data in the cloud. We have successfully implemented RBAC policy in hybrid cloud. Hybrid cloud consists of private cloud and public cloud. In this system we have created five roles for the organization ie.Role Hierarchy consist of following. SA is a system administrator that has the authority to generate he keys for users and roles, and to define the role hierarchy. RM is a role manager who manages the user membership of a role. Owners are the parties who want to store their data securely in the cloud. Users are the parties who want to access and decrypt the stored data in the cloud. Cloud is the place where data is stored and it provides interfaces so all the other entities can interact with it.

Private Cloud Module:

In this paper we have created 2 applications in our project one is for admin side and another is for user side. We have deployed these two applications successfully on this server, for deploying these two applications we have created two servers and deploy this two application successfully on this server. First we will go through the private cloud which is for the administrator and role manager of the organization. The application which is developed for private cloud which will be accessed by only by the administrator and role manager of organization.

Public Cloud Module:

As from the proposed system application which is developed for the public cloud will be access by the user, here user may be the part of organization or he may be external party. Now if any users who want to upload the file to particular role.

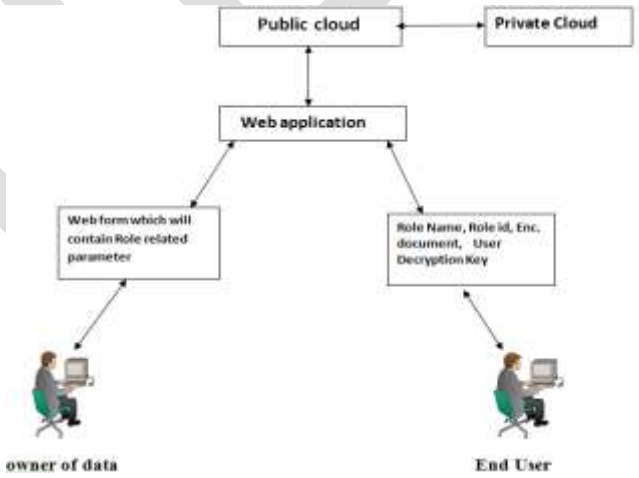

Fig3. Access to Application

As shown in Fig2.Flow of the system flow will be as follows.

Role manager will generate the different role and id related to that role and will upload this data to the private cloud. Then administrator of the organization will add different role and user to different role and will generate user decryption key. This generated user decryption key will be send to the user via mail or text message. Only admin will have access to the private cloud. Public cloud will be accessed by the user and owner of data. As shown in fig the owner who wish to upload the data for particular role. He will get the role related parameter on the public cloud and getting this information he will encrypt the document and will add encryption key to it. Now this encrypted document will be uploaded to the public cloud. Now when any user who want use any document he will have to satisfy the particular role if he satisfy the particular role then and only then he will get the document decryption key. From this we can conclude the size of the cipher text remain same although the number of user increases.

A. Owner of data

As shown in fig3. We can see that owner may be the external user or within the organization. When he wants to upload the document in encrypted form in cloud he will add the following parameter.

- Encrypted Document
- Role Name
- Role ID
- Decryption key of Document

After this document will be in encrypted form and all the secure information will be stored on private cloud.

B. User

Now when the owner of data upload the file to the cloud The User who wish to use that file or want to decrypt the file ,he must have the decryption key of that particular file then and only then he will be able to decrypt the file. When he wants to decrypt the file he will have to enter the following parameter

- Role Name.
- Role Id.
- User Decryption key (dk).

All the information enters by the use will be verified at private cloud. If all the information which is passed or entered by user is true or verified then he will be given the decryption key of the file. If that user decryption key is not present then user will not be given the file decryption key.

System Evaluation:

We come to following conclusion when the different operation is performed on the system.

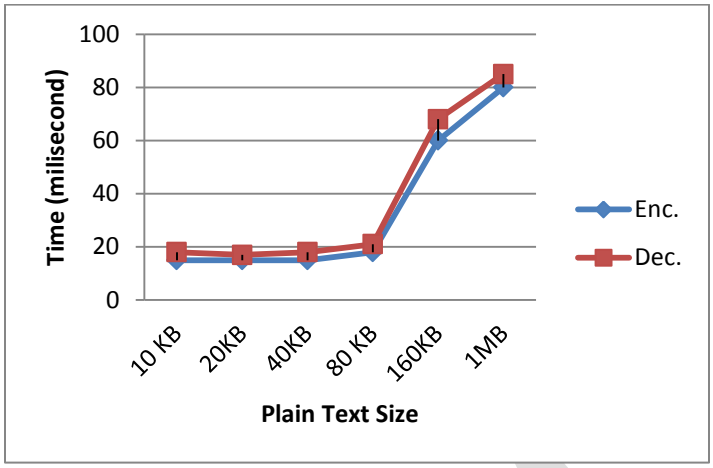

Fig4. Response for Different size

From the above graph it can be observed that system is taking same time for encryption and decryption time when the size of document is same. But time is increasing for both encryption and decryption operation when the size of the document get increase.

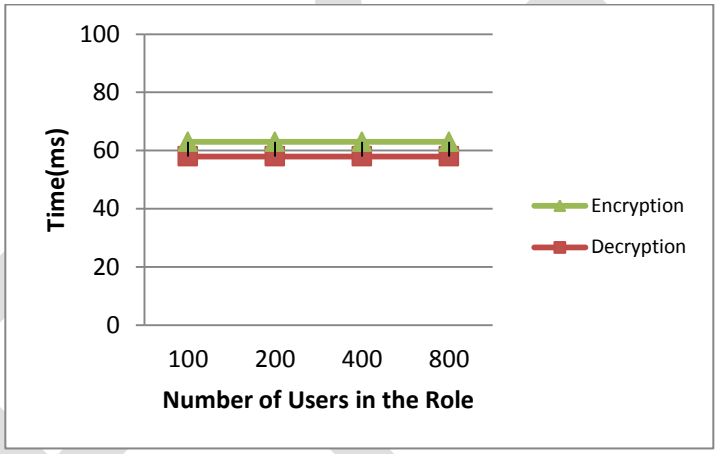

Fig5. Response for Different number of user

From the above graph it can be observed that response for encryption and decryption time is same regardless of the no user existing in the system.

5. APPLICATION

This policy can be implemented in any organization where role hierarchy plays an important role .The organization which wish to upload the document to the cloud with security .This policy provide the full security to the documents. This project can be used in colleges or company need to provide the access to the file to appropriate role and to user .As we know that there exists the different role and user in these organization and can be implemented easily.

6. CONCLUSION

As from the previous studies we can understand that the current system have lots of drawbacks. And from the Literature studies we come to understand that, there is insecurity to the document or data which is uploaded to the cloud. So, to overcome some of these drawback we have develop this project i.e. Implementation of Role Based Access Control on Encrypted Data in Hybrid Cloud which is the great improvement over previous system. The RBAC policy in Hybrid Cloud system was thoroughly checked and tested with dummy data and thus is found to be very reliable and user friendly. And it is also checked that weather is following the mapping Data to user and user to role. In this we have checked all the condition and it observed that it satisfy all the condition which was assume to be follows.

ADVANTAGES

- It is fast, efficient and reliable
- Avoids data redundancy and inconsistency
- Size of the cipher text remain constant regardless of no of user and roles.
- Provides more security and integrity to data

7. ACKNOWLEDGEMENT

I would like to express my deep and sincere thanks to Prof. A. B. Deshmukh and Co. guide Prof. M.D.Tambhakhe for their unstinted support and valuable guidance directing the course of action in the necessary and new direction and imparting me the knowledge to work satisfactory and to be able write and present this report. I would like to express my sincere thanks to our principal Dr. S. A. Ladhake for giving their valuable support. I am also thankful to Head of Department (IT) Prof. Dr. V. S. Gulhane for providing their support and necessary facilities, without whom this work would have been a goal at infinity.

REFERENCES:

[1] C.Blundo, S. Cimato, S.D.C.di Vimercati,A.D. Santis S. Foresti, S. Foresti, S. Parabosch, et al.,"Efficient key management for enforcing access control in outsourced scenarios," in SEC(IFIP), vol. 297. New York, NY, USA:Springer – Verlag, May 2009, pp. 364-375

[2] H. R. Hassen, A. Bouabdallh, H. Bettahar, and Y. Chllal, "Key management for content " Access control in hierarchies," Comput. Netw. vol. 51, no 11, pp. 3197 – 3219, 2007.

[3] http://searchcloudcomputing.techtarget.com/defination/hybrid-cloud.

[4] L. Zhou, V. Varadharajan, and M. Hitchens, "Enforcing role-based access control for secure data storage in the cloud," Comput. J., vol. 54, no. 13, pp. 1675–1687, Oct. 2011.

[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. H. Katz, A.Konwinski, et Al., "A view of Cloud Computing ," Common. ACM, vol. 53, no. 4, pp. 50-58 2010.

[6] M .J. Atallh, K. B. Frikken, and M.Blanton, "Dynamic and efficient keymanagment"For access control in hierarchy," Computt.Netw. Common. Sec., Nov. 2005, pp. 190-202.

[7] P. Samarati and S. D. C. di Vimercati, "Data protection in outsourcing scenarios: Issues and directions," in Proc. ASIACCS, Appr. 2010. pp. 1-14

[8] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security fromidentity-based Encryption,"in EUROCRYPT (Lecture Notes in Computer Science), vol.3027.New York, NY, USA: Springer-Verlag, 2004, pp.207-222.

[9] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati,"Over Encryption: Mangment of access control evolution on outsourced data," in proc. VLDB, Sep. 2007, pp. 123-134.

[10] S. G. Akl and P.D. Taylor, "Cryptographic solution to problem of access control in HierarchyTrans," ACM Trans. Comput. Syst., vol. 1. No. 3, pp. 239-248, 1983.

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data Access control in cloud computing," in Proc. IEEE INFOCOM, Mar 2010,pp.534-542.

[12] Y. Zhu, H.Hu, G. –J. Ahn, H. Wang and S.-B Wang, "Provably secure role–based encryption with revocation mechanism," Comput. JSci Techno vol 26, no. 4, pp. 697 -710, 2011.

[13] Lan Zhou, Vijay Varadharajan, and Michael Hitchen "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013