Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.384 – 390

RESEARCH ARTICLE

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

Gajanan Ganorkar[1], Anand Deshmukh[2]

[1]Information Technology & S.G.B.A.U. Amravati, India

[2]Information Technology & S.G.B.A.U. Amravati, India

[1] g.ganorkar7691@gmail.com; [2] abd_07@rediffmail.com

Abstract— Cloud System provides an efficient way for storing the large amount of user's data on the cloud. Due to this reason there has been growing trend to use the cloud for storing the large amount of data. This has raised the important security issue of how to control and prevent the unauthorized access to data which is stored on the cloud. One well known access control model is the Role Based Access Control (RBAC), which provides flexible controls and management by having two mapping, User to Role and Role to Privileges on data. RBAC is a well known access control model which can be used to protect the security of the cloud data storage. Although this cryptographic RBAC scheme have been developed recently to secure data which is outsourced by the owner of data on the cloud , but this scheme assumes there is existence of a trusted administrator who is managing all the users and the roles which is not realistic in large scale system. In this paper work we are going to implement the Role Based Encryption (RBE) scheme which can be efficiently implemented with the Role Based Access Control for storing the data on cloud securely. Based on the proposed scheme we present a secure RBE-based hybrid cloud storage architecture that allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud Also the size of the cipher text remain 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— Hybrid 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. As we know that there are different infrastructure 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 [4]. 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 paper we are going to address the issue of storing the data on public cloud securely. Public cloud is formed by two or more data cantered 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 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 [12] 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 data that owner has uploaded to the public cloud.

As shown in fig.1 We can see public cloud is accessible to any user because data centre of public cloud can be located anywhere user will never know where his data is stored in opposite to 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

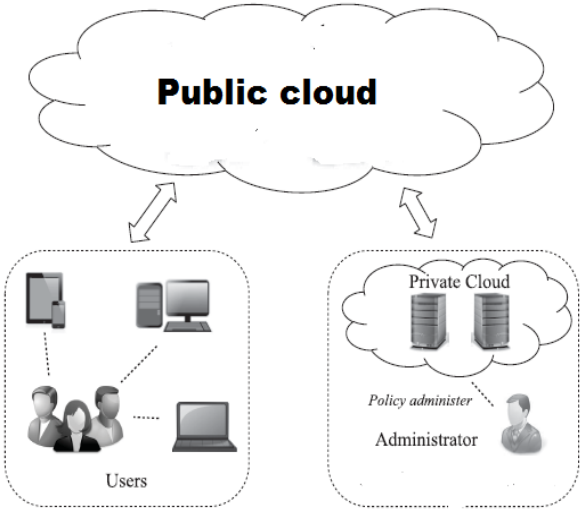

Fig. 1 Hybrid Cloud storage

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 enters, there may not be a single central authority which controls all the data centres. 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 an broadcast encryption1 mechanism described in [5]. In our 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. Our 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 a

role 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 develop 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 store only the organization's sensitive structure information such as the role hierarchy and user membership information, and the public cloud is used to store the actual data that is in the encrypted form. The high level architecture of the hybrid cloud storage system is illustrated in Fig. 1. 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. This architecture not only dispels the organization's concerns about risks of leaking sensitive structure information, but also takes full advantage of public cloud's power to securely store large volume of 1A broadcast encryption scheme is an encryption scheme where messages can be encrypted and securely broadcast to a group of users who are listening in a broadcast channel. Another significant benefit of this architecture is that it overcomes collusion attacks such as the public cloud colluding with a revoked user, thereby allowing this user to decrypt data that has been encrypted to a role of which the user was member previously. 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. LITERATURE REVIEW & RELATED WORK

There exist many hierarchy access control scheme [2], [5] ,[9] 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], [8] ,[6]. But this scheme has disadvantaged 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 is by trusted parties which are usually service provider. As we know that in public cloud data can be distributed at different data centre. Furthermore the when the 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.

III. ANALYSIS OF PROBLEM

As we know that in previous system there was some disadvantage of the traditional system i.e. key management also if the user has removed from the user revocation still he has key to decrypt the file .To overcome this situation we have proposed the RBE scheme which can be efficiently used with RBAC scheme. Also the size of the cipher text remains constant if the no. of user increase. 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.

A. System 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.

B. 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

C. Owner

Owner will have direct access to the public cloud. Owner may be the external user or user within the organization who wish to encrypt the data for users of particular role. When he will encrypt particular document he will add decryption key (document key) and will add role related parameter to it. After this all the secure information will be stored into the private cloud and encrypted document will be stored into the public cloud.

D. User

User will have direct access only to public cloud , he will not be able to access the private cloud .User who want to decrypt the particular document he will have to provide the his decryption key and encrypted document .His decryption key will be verified if it is present then and only then he will be given the decryption key of the document by using which he will be able to decrypt the data and will be able to see the original content of the document which was in encrypted form in public cloud before the decryption.

IV. PROPOSED SYSTEM

In this paper we are going to implement the web application as shown in fig

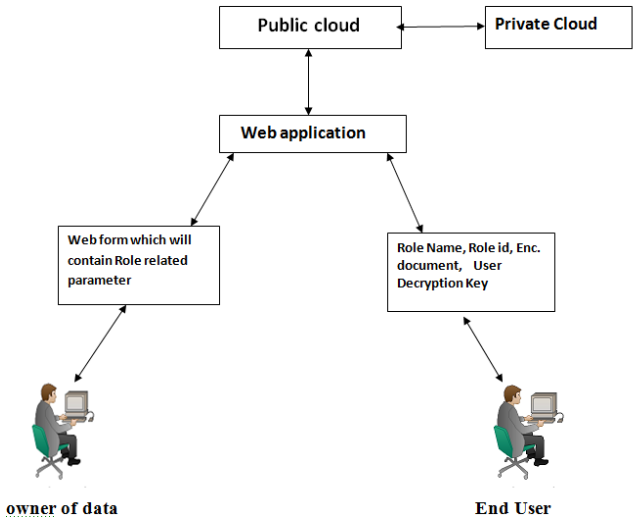

Fig. 2: Access to application

As shown in fig. 2 we are going to implement the web application in which user and owner will have direct access to the public cloud. The entire role related public parameter will be available on the public cloud. Owner who wishes to encrypt data for particular will encrypt the document and will upload encrypted document to public cloud .Now security related information of the document will be stored on the private cloud. Whenever any valid user of particular role want to decrypt data will send the required information as shown fig after the verification is done he will be provided the document decryption key by using which he will be able to see the original content of the document.

A. Owner of data

As we said 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 enter by the use will be verify if t all the information which is passed be user is true or verified then he will be given the decryption key of the file

C. Report Generation

Admistrator can generate the report based on the different role ie .if he wished to see the all the user to particular role the he will able to generate the report. Also if he wishes to know which document is accessed by the user based on this he will be able to generate report. The different report will be generated based on the different condition.

D. Facilities

As we know that admistrator is generating the user decryption key and sending to the user via email or message .If user forgot the password or may delete the message or email then if he request for the key the again key will be provided to him via email or msg.Now if any new user has wish to add to the particular role then he will fill the form and this information will be send to the admin then admin will verify all the information if he satisfy then he will be added to the particular role our proposed system will be as showed in fig. from the fig we can see the role manager and administrator of organization has only direct access to private cloud.

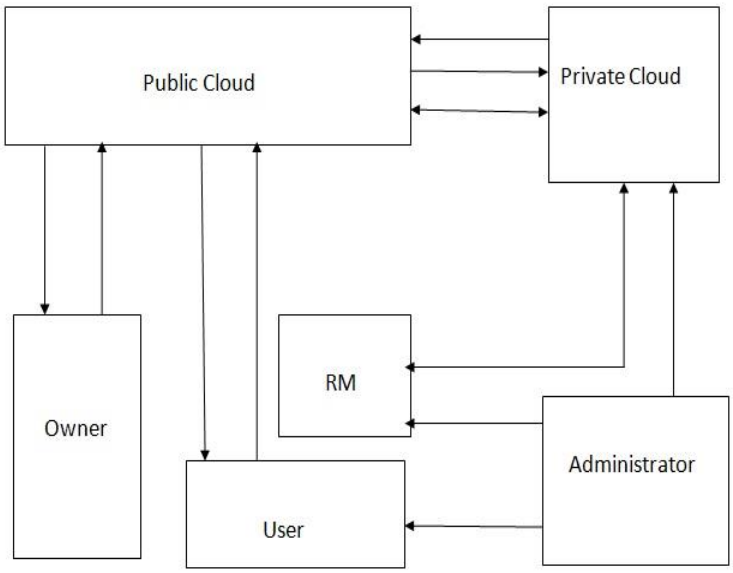

Fig. 3: RBE system

Owner and user will have direct access to public cloud they will not be provided with any access to private cloud as private cloud contain security related information about role hierarchy and user and document key so these information need to be kept secret so they have not access to it.

E. Flow of work

As shown in fig. 3 . Flow of the project 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

V. 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

VI. CONCLUSION

In this Paper, first we proposed a new RBE scheme that achieves efficient user revocation. Then we presented a RBAC based cloud storage architecture which allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. Then we will develop secure cloud storage system architecture and will show that the system has several superior characteristics such as constant size cipher text and decryption key. We believe that the proposed system has the potential to be useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these Access policies

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. 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] 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.
[4] 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.
[5] 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.
[6] P. Samarati and S. D. C. di Vimercati, " Data protection in outsourcing scenarios: Issues and directions," in Proc. ASIACCS, Appr. 2010. pp. 1-14

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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

