Enhancing Secure Access Control for Cloud Storage

Gauri Bandewar
Dept. of Information Technology
Sinhgad Technical Education Society's SKNCOE,
Pune, India
gauribandewar582@gmail.com

Prof. R. H. Borhade
Dept. of Information Technology
Sinhgad Technical Education Society's SKNCOE,
Pune, India
rhborhade.skncoe@sinhgad.edu

Abstract— **Cloud computing gives much more services to users on demand. Cloud is useful for storing large amount of data regardless of extra resources. It is necessary to provide better security when users access their data from the cloud. So that, one very useful model is RBAC (Role Based Access Control) helps in controlling access to information stored on cloud with the new concept of the hybrid cloud. This paper shows different schemes that are used to control access from the cloud. The term hybrid cloud is the composition of public and private cloud in which more sensitive information will be stored on private cloud, and all other information is stored in the public cloud but in the encrypted form. It will reduce collusion attacks. Thus, it will help to prevent unauthorized access to the cloud data to improve security.**

Keywords-Access control, cloud computing, data storage, role- based policies.

I. INTRODUCTION

Cloud storage can store large amount of data so it helpful to access it from anywhere regardless of extra resources. Three types of cloud used mainly to store information [1]. In the term hybrid cloud, there is a combination of public and private cloud. Sensitive information will store in the private cloud, and all other information will store in the public cloud in encrypted form.

Private cloud is accessed only within an organization. It is not globally accessible. There are many restrictions to access data from the private cloud. So that, private cloud is better than public cloud. Unlike public cloud, in a private cloud any external party is not allowed to access data from the cloud.

Public cloud can be easily accessible by any user. In the public cloud, users don't know where their data is stored actually because cloud is made up of various data centers and they are located in distributed manner. Therefore, unauthorized access can be made by many hackers who want to hack particular data. Public cloud may not be trustworthy. So that, to provide security in terms of data access various access control policies are developed, that can be helpful in reducing unauthorized access. Various existing systems assume that cloud is trusted. Cloud provides services at very low cost with long term archive.

Like this cloud provide three types of services. These are related to software, platform, and infrastructure. Cloud provides facility of large data storage. Any user can store his data on the cloud and can access it from anywhere.

In RBAC model, users can access their data based on their role according to their policy. In an organization for a particular user, there are many responsibilities are assigned to that user according to qualification. So, only user with appropriate responsibility can access part of data from the cloud. Permissions to access data are not assigned to users they are assigned to qualified roles only. One role can inherit the permissions from other role, and it is possible that one role have multiple users. Thus, role hierarchy of users is maintained in RBE system.

This paper is organized as follow: In Section 2 existing work is describe in detail. Section 3 introduces proposed work. Section 4 concludes the paper.

II. EXISTING WORK

A. RBE(Role Based Encryption) scheme with RBAC Policies

In RBE with RBAC Policies, hybrid cloud concept is used with RBAC model. It will helpful only when the cloud is trusted. Users with appropriate role can only access the part of data from the cloud. RBE system is based on position of a user within an organization. The scheme is useful for trustworthy cloud [1].

B. IBBE (Identity - Based Broadcast Encryption)

In IBBE scheme message broadcasting is used. This scheme first encrypts the message and after that broadcasts it to multiple users. Broadcaster is responsible for broadcasting messages. After this users use their private key to decrypt and view the data. Key encapsulation mechanism is used here [2].

C. CACH (Content Access Control in Hierarchy)

CACH scheme includes Independent and dependent key approaches. For data access, there is no need of key with which it is encrypted. Users can use their own key with some public parameters. But in independent key approach, user must have the copy of that key with which data is encrypted. But these are complex techniques [3].

D. HIBE (Hierarchical Identity- Based Encryption)

The HIBE scheme can provide secure encryption system with short size keys. This scheme uses Diffie-Hellman inversion assumption [4].

E. HKM (Hierarchy Key Management)

Hierarchy key management scheme provides adjustment of hierarchy of various keys. In HKM system, one user can be added to multiple roles also. Cipher-text size is constant. Revocation of one user will affect on another user in the same role [5].

TABLE1. LITERATURE SURVEY

Sr. no	Existing Method	Advantages	Disadvantages
1	RBE(Role Based Encryption) for resource encryption	-Support flexible encryption of resources. -Revocation is done in a min. cost. -It is scalable.	-It does not support encryption, signature, authentication
2	IBBS(Identity-based broadcast scheme)	-It has better efficiency.	-It does not allow stronger security notion equivalent to IBS.
3	Base model on selective encryption	-It allows selective access to be enforced by a service provider itself.	-It does not work well when resources are large & distributed in selective way.
4	RBE(Role-based encryption)	-Constant size ciphertext. -Constant size keys in single & multiple roles.	-User revocation affects on others. -Need of Re-encryption after user revocation.
5	HKM (Hierarchical Key Management)	Constant size cipher text -Constant. Size key in a single and multiple roles.	Revoking of user will be affect on other users. -Re-encryption is must after user revocation.
6	ABE(Attribute Based Encryption)scheme	-Secure access.	-key size is not constant. -User revocation affects on other users and roles.
7	RBE using RBAC model	-Constant size ciphertext and keys. -User revocation does not affect on other roles or users. -There is no need of re-encryption after user revocation.	-It can not identify the source of data -Data searches are not secure -This scheme does not work for un-trusted cloud.

F. RBE(Role Based Encryption)

This scheme is applied to public cloud. In this data access is based on position of that user in the organization. In this if multiple users are present in single role then any user can be added or removed from that role at any time [6].

G. Base model on selective encryption

In two-layer method, one encryption is done by owner and second encryption by service itself. This can help in providing efficient solution. This system allows selective access without owner's permission [7].

H. ABE (Attribute Based Encryption) scheme

In this system set of attributes are used in order to access data from the cloud. Set of attributes are associated with no. of ciphertext [8].

I. HIDE (Hierarchical ID-Based Encryption)

This HIDE scheme is helpful in reducing ciphertext expansion. It distributes the workload by transmitting keys. Authentication and key transmission is done locally. It also helps in damage control [9].

J. IBSC (Identity-Based Signcryption)

This scheme is proposed for efficiency purpose. Bilinear mapping are done in this scheme. In this IBS (ID Based Signature) is proposed. The IBS mechanism is faster at a verification process [10].

K. CCA- secure public key encryption scheme over IBS

In this sender first encrypt the message by use of key pair with identity. And at last cipher-text is signed with a verification key. At the time of decryption, signature is verified with the help of a verification key, and secret key is derived. In this manner, cipher text is decrypted [11].

III. PROPOSED WORK

Many RBE schemes were implemented earlier. All are very useful, but they don't provide better security in case if cloud is un-trusted. The new RBE mechanism will reduce this drawback. It includes six important components. They are owner, user, admin, role manager, public and private cloud.

Owner is only responsible for outsource data on the cloud. He is also responsible for giving access the part of data to the authorized users only. Owner will upload encrypted data with the signature for the purpose of better access control.

Role Manager can manage the roles of users. Role is based on parameters of user membership, and those parameters are stored in the private cloud. If Role Manager wants to update user membership, then he has to update it in the private cloud.

Admin is responsible for generating and computing parameters for the users. Role parameters define the position of a user in the role hierarchy. Role Manager is also responsible for the management the of a role hierarchy in the organization. Admin is allowed to update parameters in the private cloud if necessary.

User is the entity who wishes to access their data from the cloud. Upon successful authentication of user one secret is given to the user. After receiving the key, authorized user is then able to decrypt that data with the help of that secret key.

Private cloud is that which contain user's identity related information along with role parameters of that user. Information in the private cloud is sensitive information. So, it will not be accessed by any external party because the private cloud only accessed by those who are within the organization only. Unlike private cloud, public cloud is globally accessible. It exists outside the infrastructure of the organization. Any unauthorized party is also able to access the data from the cloud.

A. Comparison between existing RBE and RBE using SHA-512

In previous RBE system, authentication of a user is provided that is not so efficient and whole concentration is given on securing access control only. It is necessary to provide better authentication to increase access control. But in RBE system, if SHA algorithm is used then it can help in providing better authenticity. SHA is a Secure Hash Algorithm. With the help of this SHA-512 algorithm, signature can be generated and based on this signature any authorized user will be identified. Owner will verify the signature and grant access to only those users who are authorized or who will match that signature. For greater authentication purpose SHA-512 algorithm will be used, and all other access is based on role parameters of a user.

B. Steps for RBE scheme

Step 1: Owner outsources the data to the cloud in encrypted form with attached signature.

C=(Enc(M),Pk), Signature

C= cipher-text
M= Plain-text

Step 2: Role Manager can add or revoke user by granting or revoking permission to the user of IDu. He then updates (List of User Role) of that role in the private cloud.

AddUser=(Pk, LURr,IDu)

RevokeUser=(Pk,LURr,IDu)

Step 3: User wants to access data from the cloud. Owner authenticates user with identity of that user and allow him to access data if,

ID=IDu

Step 4: Role Manager validates user based on role parameters and identity of that user.

Step 5: User view that data by decrypting it with a decryption key and get an original message.

M=(Dec(C),Pk))

This paper proposes RBE scheme that applied with the help of SHA-512(Secure Hash Algorithm) and RSA (Ron-Rivest Shamir Adleman) algorithms. For generating hash code on the sender side and receiver side SHA-512 algorithm is used. The method is simple. In the proposed system, when owner uploads the data on the cloud, he must attach his signature to it, and also he has to encrypt that information before outsourcing to the cloud. For the sign generation at encryption side and verification at decryption side, SHA-512 algorithm is used. Any authorized user wants to access data from the cloud or want to modify his data then he makes a request to the owner. Owner first authenticates the user and Role Manager checks the membership of a user within an organization and then gives appropriate access to that user. This concept will help in controlling access from the cloud that result in secure searches. Many existing schemes do not perform well in the case when cloud provider is un-trusted. But in new RBE approach that problem can be reduced by using the concept of the hybrid cloud. New RBE mechanism helps in providing better authenticity. It includes RSA algorithm to provide better authenticity. If any unauthorized user will access data from the cloud, then this will be avoided in new RBE system by giving associated decryption key to the authenticated user so unauthorized access will be reduced even it also helps in reducing misuse of data. This scheme gives complete focus on access control and authenticity.

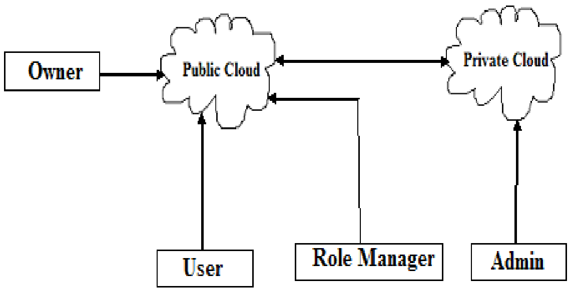

Figure1. Cloud Storage Architecture

IV. CONCLUSION

Cloud computing has several benefits regarding storage capability. It can handle a tremendous amount of data. To secure data that is present in the cloud, several access mechanism are developed. These are useful for securing data access from the cloud. To prevent attacks access control mechanism is necessary SHA-512 algorithm can help to minimize unauthorized access to the cloud. In trusted cloud, many security policies can be applied for securing data. So that, it is necessary to focus on to secure data when the cloud is un-trusted.

ACKNOWLEDGMENT

I would like to thank my guide Prof. R. H. Borhade for his exemplary guidance and constant encouragement throughout the duration of the paper. His valuable suggestions were of immense help throughout this paper. I am also thankful for the concern members of iPGCON2015 for their constant guidelines and support.

REFERENCES

[1] L. Zhou, V. Varadharajan, and M. Hitchens, "*Achieving Secure Role- Based Access Control on Encrypted Data in Cloud Storage*", IEEE TRANSACTIONS ON INFORMATIONFORENSICS AND SECURITY, VOL. 8, NO. 12, DECEMBER 2013.

[2] Cecile Delerablee, "Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private Keys", ASIACRYPT 2007, LNCS 4833, pp. 200–215, 2007.
[3] H. R. Hassen, A. Bouabdallah, H. Bettahar, and Y. Challal, "Key management for content access control in a hierarchy," *Comput. Netw.*, vol. 51, no. 11, pp. 3197–3219, 2007.
[4] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity- based encryption with constant size ciphertext," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494. New York, NY, USA: Springer-Verlag, May 2005, pp. 440–456.
[5] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies," in *Proc. ACM Conf. Comput.Commun. Sec.*, Nov. 2005, pp. 190–202.
[6] 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.
[7] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proc. VLDB*, Sep. 2007, pp. 123–134.
[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Sec.*, Oct./Nov. 2006, pp. 89–98.
[9] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in *ASIACRYPT* (Lecture Notes in Computer Science), vol. 2501. New York, NY, USA: Springer-Verlag, 2002, pp. 548–566.
[10] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably secure identity based signatures andsigncryption from bilinear maps," in *ASIACRYPT* (Lecture Notes in Computer Science), vol. 3788. New York, NY, USA: Springer-Verlag, Dec. 2005, pp. 515–532.
[11] R. Canetti, S. Halevi, and J. Katz, "Chosen-ciphertext security from identity-based encryption," in *EUROCRYPT* (Lecture Notes in Computer Science), vol. 3027. New York, NY, USA: Springer-Verlag, 2004, pp. 207–222.