International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Data Security for Cloud Storage System Using Role Based Access Control

Prachi Shah

Computer Engineering, J. S. P. M, Tathawade, Pune, Maharashtra, India - 411033

Abstract: ***A cloud storage system is collection of storage servers. A Secure cloud is a reliable source of information. Protection of the cloud is a very important task for cloud service providers. Today is the need of low-maintenance system which automates administration daily and also need of access control over network so that data security is maintained and ensured. Role-based access control (RBAC) method controls access to computer or network resources based on the roles given to individual users within an organization. Roles are defined according to job skill, authority, and responsibility within an organization. In RBAC, roles can be easily created, changed, or discontinued as the needs of an organization involve, without updating the privileges for every user.***

Keywords: Role-based access control, cloud computing, role-based encryption, role-based encryption system architecture

1. Introduction

Sharing of resources on cloud can be done on large scale which is cost effective and location independent. Resources on the cloud can be deployed by the service providing person or company and used by the client. It also shares necessary software's and on-demand tools for various IT Industries. Cloud provides many advantages as storing information on the cloud gives almost unlimited storage capacity; easy access to information gives access permission to data stored on cloud from anywhere if user is registered to it. On other side, cloud got many issues regarding security especially on Data theft, Data loss and Privacy.

Protecting cloud from unauthorized users[2] and other threats is a very important task for security providers who are in charge of the cloud as secure cloud is always reliable source of information. A Cloud is said to be good only when it is reliable and provides better security to customers. Even if vendor is providing secure cloud, the vendor should make sure who can access the data and who maintains the server.

1.1 Role-Based Access Control

Role-based access control provides a better security solution for accessing data on cloud. Roles in RBAC are mapped to access permissions [4], and all users are mapped to appropriate roles and receive access permissions only through the roles to which they are assigned, or through hierarchical roles, roles get access permission. Within an organization, there may be number of users and types of permission, whose role and accordingly access differs. Controlling all access through roles gives benefit to organization and it also simplifies the management.

Typically, role-based access control model has three essential structures; users permissions and roles. A role is a higher level representation of access control. User correspond to real world users of the computing system. User authorization can be accomplished separately; assigning users to existing roles and assigning access privileges for objects to roles. Permissions gives a description of the access users can have to objects in the system and roles gives a description of the functions of users within an organization. In RBAC, there is hierarchical structure; a role can inherit access permission from another role. Following diagram shows relationship between users, roles and permissions.

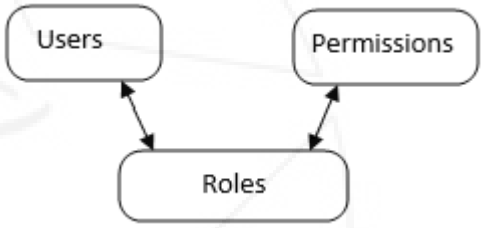

Figure1: Relation between users, roles and permissions

Data owner uses cryptographic techniques to protect data from unauthorized access for providing protection to the privacy of their data and only those users can access data who have access permission. Users need to satisfy access policies to access data. If user satisfy the access policies, user can decrypt data by using his private key. The role based access policies are strengthened by using role-based encryption scheme (RBE).

1.2 Role-Based Encryption

In RBE scheme [1], the owner of the data encrypts the data in such a way that only those users can decrypt the data who possess appropriate access permission according to their role specified by role-based access control policies. Role grants permission to access data according to their role and can also revoke the permission from existing user of role. Revoked user will not have any type of access permission to any encrypted data for the role. Revocation of the user does not affect other users and roles in the system.

In RBE, four types of entities[10] are used; SA is a system administrator which generates keys to users and roles and provides authorization. RM is a role manager who gives access to user according to their role. Users used to decrypt and access data from cloud. Data are stored on cloud by owner of the data.

In RBE system, following algorithms are used; Setup(λ): This algorithm takes λ as input and generates master secrete key (mk) and public key (pk).

Extract(mk, ID): SA execute this algorithm. If user identity ID matched, then SA provides mk to the user i.e. if ID = IDu, then SA generates dku which is secrete key of user. If ID is matched with role, SA provides mk to RM i.e. if

ID = IDR, then SA generates skr which is secrete key of role.

Manage Role(mk, IDR, PRR): SA execute this algorithm to manage role with identity IDR from other role. Here, role hierarchy is maintained. All the roles are stored as a set of PRR. SA generates role public parameter as AR, BR and stored them on cloud.

AddUser(pk, skR, RULR, IDu): RM execute this algorithm in which RM gives role to user and also provides authentication. Role user list RULR is updated in cloud.

RevokeUser(pk, sk, RULR, IDu): RM execute this algorithm and sends user ID IDu to the cloud, then cloud computes some parameters and send them back to RM from which RM replaces old role parameters with new parameters.

Encrypt(pk, pubR): Encryption is done by owner of the data and it stores cipher text C of message m to the cloud. This algorithm takes pk and pubR as input parameters and generates (C, K) tuple where K is used to encrypt original message.

Decrypt(pk, pubR, dku, C): This algorithm is executed by those user who possess access according to their role. This algorithm takes pk, pubR, dku, C as input parameters and generates output by decrypting original message by using K.

Security information can be attached to a network object as a list, recording a group of trusted network objects that are authorized to access other network objects. This is an Access Control List (ACL). Permission is a set of attributes describing the kind of privileges that determine what a network object can do. The administrator assigns permissions to a network object. A permission[4][6] set contains only the following privileges:

Supervisor (S) grants all sorts of rights to an individual network object or group of objects

Create (C) allows the creation or renaming of a network object

Delete (D) enables the deletion of a network object

Read (R) allows a network object to read the content of an object value

Write (W) lets a network object write or modify the content of an object state

Execute (X) enables a network object to execute services (or operations) of other network objects.

RBAC policies [5] include role hierarchy, role hierarchy with private roles, separation of duties chinese wall policy, delegation, joint action based policies, limiting number of accesses.

Role hierarchy – This gives hierarchical ordering of responsibilities with more senior positions encompassing all the privileges of the more junior positions, plus some extra privileges.

Role hierarchy with private roles – in this type, not all privileges are inherited. Privileges may need to be shared amongst all holders of a position, but not inherited or may require privileges to be private to individual users.

Separation of duties - Different types of group of users performed different types of actions on objects.

Chinese wall policy - In this policy, objects are grouped together into different sets which reflect conflicts of interests. If a user has accessed an object in a set, then the user is not allowed to access any other object within that conflict of interest set.

Delegation – Delegation is handled by assigning and de-assigning roles. When the delegation actions performed, roles are removed.

Joint action based policies - Joint action based policies are used in situations where trust in individuals needs to be dispersed. joint actions agents may acquire privileges, by working together in tandem, which none posses in isolation.

Limiting number of accesses – one user can give access to other user with limiting the number of operation.

1.3 Role-Based Encryption System Architecture

A secure RBAC based on hybrid cloud storage[2] architecture which allows an organization to store information on public cloud and maintain sensitive information on private cloud.

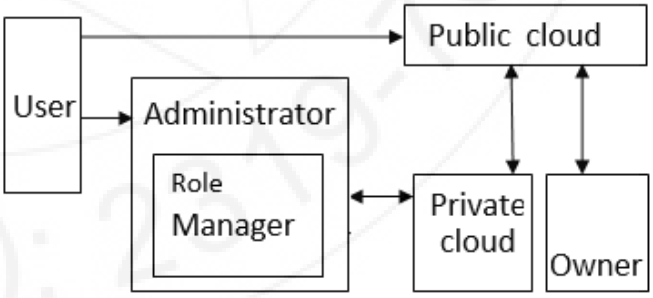

Figure 2: RBE based hybrid cloud system

Public cloud provides services in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network. Only public information and encrypted data will be stored in public cloud.

A private cloud provides a distinct and secure cloud environment in which only the specified users can access data from it. The private cloud is only accessible by a single organization, provides greater control and privacy. The

organizations stores only critical and confidential information in private cloud. The amount of information stored in private cloud is relatively small as compared to public cloud. The private provides interfaces to the role manager, administrator and public cloud. Users can not access data directly from private cloud.

Users are the parties who wish to acquire certain data from the public cloud. Only authenticated users can acquire such data. Administrator of role based system provides authentication to users. If user is authorized, he then provided with secret key upon which proves identity of the user. Users are just to access data from cloud. They cannot do any modifications, updations to original data. They cannot communicate directly with the private cloud as they don't possess access permission.

Administrators generate the system parameters. System parameters represents the position of the role and stored that role in private cloud. Administrators manages role hierarchy. Role manager manages role for users. According to the role, user gets access permission to data. Each role has different parameters associated with it. These role parameters are stored in private cloud. In RBAC, owner of data are the parties who gives permissions to access their data according to roles.

2. Conclusion and Future Work

Role-based encryption scheme is proposed to achieve efficient user revocation. Role-based access control model based on hybrid cloud storage architecture in which encrypted data is stored on public cloud and sensitive information related to organization stored on private cloud, from which outside users can not access data directly. RBAC contain some privileges and access policies. Based upon authorization and access permission policies, user can access data from cloud.

3. Acknowledgement

I would like to thank my guide for his help and guidance throughout this project and the semester, without him this would not have been possible.

References

[1] Lan Zhou, Vijay Varadharajan and Michael Hitchens "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.
[2] Hsiao-Ying Lin, Wen-Guey Tzeng "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", IEEE Transactions on Parallel and Distributed System, Vol. 23, No. 6, June 2012 .
[3] Vijay Varadharajan and Michael Hitchens "Design and specification of role-based access control policies", IEEE Transactions on Information Forensics and Security, Vol. 147, No. 4, August 2002
[4] Zahir Tari and Shun-Wu Chan "Role-based access control for intranet security", IEEE Internet Computing, Vol. 1, No. 4, September 1997
[5] Pierangela Samarati and Sabrina de Capitani di Vimarcati "Access control: Policies, Models and Mechanism", 2001
[6] Vijay Varadharajan, and Allen, P.: 'Joint action based authorization schemes', ACM 30, Oper. Syst. Rev., 1996, 3, pp. 3245
[7] C. Delerablée, "Identity-based broadcast encryption with constant size ciphertexts and private keys," in ASIACRYPT (Lecture Notes in Computer Science), vol. 4833. New York, NY, USA: Springer-Verlag, 2007, pp. 200–215.
[8] 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.
[9] Y. Zhu, H. Hu, G.-J. Ahn, H. Wang, and S.-B. Wang, "Provably secure role-based encryption with revocation mechanism," J. Comput. Sci. Technol., vol. 26, no. 4, pp. 697–710, 2011.
[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, D. Ma, C. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in Proc. Int. Workshop Sec. Cloud Comput., 2013, pp. 33–40.
[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO (Lecture Notes in Computer Science), vol. 196. New York, NY, USA: Springer-Verlag, 1984, pp. 47–53.
[13] 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.

Author Profile

Prachi N. Shah, have completed Bachelor of Engineering in Computer Science from Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Sant Gadage Baba Amravati University, in 2008. She has passed Bachelor of Engineering with first class. Currently, she is pursuing Masters of Engineering in Computer Science and Engineering from J.S.P.M`s Rajarshi Shahu College Of Engineering, Savitribai Phule Pune University, Tathawade, Pune. She is doing research on "How to use Role-Based Access Control to provide data security in cloud storage system".