A Review of Role based Encryption System for Secure Cloud Storage

Avdhut Suryakant Bhise
M.E. Student
JSPM's ICOER Wagholi, Pune

Phursule R.N.
Asst. Professor, Dept. Of Information Technology,
JSPM's ICOER Wagholi,Pune

ABSTRACT
There has been a growing trend to use the cloud for large-scale data storage. It has raised the important security issue of controlling and preventing any unauthorized access of data stored in the cloud. The role-based access control (RBAC) one of the well known access control model provides flexible controls and management by providing two mappings, one by mapping users to the roles and another by roles to the privileges on the data objects. In this we will discuss a role-based encryption (RBE) scheme that has been used previously with RBAC. A hybrid cloud storage of the RBE scheme architecture permits an organization to store data secure in a public cloud and maintains the private information related to the organizational structure in a private cloud. In this we will also focus on the models that are available in cloud computing.

General Terms
Cloud Computing

Keywords
Role Based Access Control (RBAC), Role Based Encryption (RBE). Access Control Models, Attribute-based Encryption Model, Multi-tenancy Model.

1. INTRODUCTION
Effective and secure information sharing, especially across multiple cooperating yet mutually suspicious organizations, is a fundamental challenge in today's information-rich and information-dependent society. The necessity to share but protect is among the oldest challenges for trustworthy computing. There has been a growing trend in the recent times to store data in the cloud with the dramatic increase in the amount of digital information such as consumers' personal data to larger enterprises wanting to back up databases or store archival data. Cloud data storage can be attractive for users with uncertain storage demands, requiring a cheap storage tier or a low cost, long-term archive. By outsourcing users' data to the cloud, service providers can focus more on the design of functions to improve user experience of their services without worrying about resources to store the growing amount of data. However, several recent surveys [2], [3] show that 88% potential cloud consumers are worried about the privacy of their data, and security is often cited as the top obstacle for cloud adoption. There are different types of infrastructures associated with a cloud [4]. A recent survey [5] shows that nearly half, 43% of all companies report utilising private clouds and 34% of companies say they will begin to use some form of private cloud in the next six to twelve months. a secure RBAC based cloud storage system where the access control policies are enforced by a new role-based encryption (RBE). This RBE scheme enforces RBAC policies on encrypted data stored in the cloud with an efficient user revocation using a broadcast encryption mechanism described in [5]. RBE 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 new RBE scheme, 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 approach [1], RBE scheme achieves an efficient decryption on the client side. This also uses 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, develop a secure cloud data storage architecture using a hybrid cloud infrastructure. In RBAC, a user will have access to any object according to his/her assigned role in the system. The roles are assigned according to the job functions. Permissions are assigned on job authority and responsibilities according to the job. Operations on the given object will be invoked based on the permissions assigned to the job authority. RBAC models are more flexible than the other access control models such as discretionary and mandatory models, and this model suits for use in cloud environments, especially for the services for the users cannot be tracked with a fix identity. The paper mainly focuses on the following three categories of control models for cloud computing these are: 1] Role-based 2] Attribute-based encryption and 3] Multi-tenancy models. The paper provides review of this existing literature on each of the above access control models and their variants (with technical access, aspect and relevancy). Due to which we can identify future research directions for creating access control models for cloud computing environments which will be more effective.

2. LITERATURE REVIEW
Role-based Access Control (RBAC) was first addressed by Ferraiolo and Kuhn in [6] to show the limitations of discretionary access control model (DAC). Sandhu et. al [7] addressed 4 reference models for providing systematic ap-proach to understand RBAC model. Their framework sep-arates administration of RBAC from its use for controlling access. They also categorize the implementation of RBAC in different systems. Finally, after a series of modifications, the NIST standard for RBAC is proposed in [8]. The standard specifies RBAC reference model which defines the scope of a feature that comprise the standard and provides terminologies to support specification. The standard also specifies system and administrative functional specification which de-fines functional requirements for administrative operations. In [9] the authors present a history-based access control mechanism which is suitable for con-trolling access of mobile code. The scheme will maintain a history of selective requests made by individual program and will use this to measure the degree of safety of a given request. One another history based access control for the codes is presented in [10]. The access

privileges of a code are determined dynamically by examining the behaviour of the pieces of code that have executed before. The piece of code that have executed include the codes on stack as well as the codes that have been called and returned. Sandhu et. al in a recent paper [12] present a trusted computing architecture to enforce access control policies in peer-to-peer environment.

The comparison of the existing schemes which can be used to enforce RBAC policies and proposed scheme is shown in Table 1.

Table 1. Comparison of schemes for enforcing RBAC policies

	HKM	**HIBE**	**ABE**	**Proposed scheme**
Constant size cipher text	√	√	–	√
Constant size keys when a single roles	√	–	–	√
Constant size keys when a multiple roles	√	–	–	√
User management delegation	–	–	–	√
Revoking users not affecting other users/roles	–	–	–	√
No need revocation after user revocation	–	–	–	√

3. ROLE BASED ENCRYPTION (RBE) SCHEME

In 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. The RBE 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 RBE scheme, revocation of a user from a role does not affect other users and roles in the system. In addition, RBE outsources part of the decryption computation in the scheme to the cloud, in which only public parameters are involved. By using this approach, RBE scheme achieves an efficient decryption on the client side. The same strategy of outsourcing to improve the efficiency of the management of user to role memberships, involving only public parameters.

4. ACCESS CONTROL MODULES FOR CLOUD

4.1 Role Based Access Control Model

In a RBAC model, the user role is assigned based on the authority – the role with the least permissions are necessary for the completion of the job. Task Role-based access control model (TRBAC) [11] has been a model for cloud computing environments [13] where the regular static access control models such as alternative, important or simple role based models cannot be employed. TRBAC could dynamically check the access authority for users based according the given roles and the job the user has to perform according to the given role [22]. Tasks could be classified as planned task (those are needed to be completed in a specified order) will need active access control and non-planned tasks (those are can be completed in any order) will need passive access control. The tasks which are planned tasks are active role based access control is time constraint and the access authority assigned for users performing the tasks change at run time, it depends on the order the tasks are to be executed. It should make sure that a user will have the minimum required access to perform a task under a certain role and the role cannot be assigned to two or more tasks at same time. An alternative of role based access control for cloud environments is the Attribute role based access control (ARBAC) model [14], where the data objects which are protected will be assigned with specific attributes and values. The authorized user with a certain role has to provide the proper values for these attributes, and after proper validation by the service provider access will be given to the objects. A key based fine-grained ARBAC has proposed in [15], where users will have assigned with private keys that are used for encrypting or decrypting the values of the attribute defined for the objects whose secrecy needs to be secured. The access authority for a user or role is based on the threshold. The trust level established based on the requestor's access. If the user differs from his or her profile, then trust for that user will be automatically decreased to avoid potential violence of rights. Bertino et al [16] projected the temporal RBAC (TRBAC) model that allows and disallows a role at run time according to requests of users. In [17], in some applications, certain roles need to be constant and stay enabled all the time, while there only the users and permissions that are going to be assigned dynamically. Another generalized model is also projected called TRBAC model that look for activation of role instead of role enabling. It will be activated if at least 1 user assumes that role.

4.2 Attribute Based Encryption Model (ABE)

Attribute-based encryption is more suitable to protect the confidentiality and secrecy of data in a cloud. It is useful for the source of the data that unknown of the personality of the receiver and their public key; it only knows certain attributes of the receiver. ABE identifies a user with a set of attributes. Two variants are proposed in the literature as an extension of ASE: Key Policy based ABE (KP ABE) scheme and the Cipher Text Policy based ABE (CP ABE) scheme. In KP ABE [18], the key is related with the access tree and the cipher text is related with an attribute set. The encrypting party will not have control for users who are going to access the data and it can define the set of attributes necessary for decrypting the cipher text. In CP-ABE [19], the cipher text is related to the access tree and the owner will determine the policy for decrypting the data, the key is related with a attribute set.

In [20], author suggest a multi authority ABE based control model which suits for cloud computing. According to this, every user is provided with a unique global user identifier (UID) and a unique authority identifier (AID). Both these will be provided by a certified authority (CA) believed by the various controllers of the domains. To prevent two users from intrigue together to get illegal data access, the CA certified UID is added together with the secret key issued by various domain authorities for decrypting data. A well-organized attribute revocation method in multi authority CP ABE system is now using alternate encryption. The CA based scheme is dispersed more than the KDC based approach. Also the KDC needs to be always online for distributing keys to users, whereas a CA need not be online always.

4.3 Multi Tenancy Model

A central system to globally administer right to use control can engage a bigger number of permission rules that increased significantly with increase in the crude of resources, also through the number of users and services provided by the cloud. The cloud computing demands a unreliable degree of granularity in access control systems due to the heterogeneous services provided, so there is a requirement for local independence imply that each service model keeps administrative control over its resources. In [21], the authors recommend a hypervisor based multitenant access control mechanism called Cloud Police and say that such an approach for cloud is more reliable and tough than the network based techniques. Hypervisors are having full programmability of the software; as well they are trusted, network independent and they can also block unwanted traffic before reaching the network. For facilitating hypervisor-based access control policies, one could predict several solutions. A best solution would be to install all the policies and the entire mapping between the Active Virtual Machines (VM) and groups in all hypervisors, so a source hypervisor can directly apply the policy of the destination to all the flows sent by its hosted VMs. However, applying this approach is not scalable. Another best solution is to employ the centralized repository for the policies and group membership is that hypervisors will have to check with this repository to prefer on each new flow and possibly cache the access control policies. Such a centralized service has to bear high accessibility and low reaction time also it is likely to be a intention for the denial of service attack. Another way to handle scalability is to have hypervisors in cloud to organize and setup according to the access control plan of the hypervisors of the destination VMs to hypervisors of the source VMs.

5. ACKNOWLEDGMENT

I thank to my respected guide Prof. R.N. Phursule (Asst. Professor, Dept. Of Information Technology) for his valuable guidance.

6. REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[2] 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.

[3] 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.

[4] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Trans. Comput. Syst., vol. 1, no. 3, pp. 239–248, 1983.

[5] 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.

[6] D. Ferraiolo and R. Kuhn. Role-Based Access Controls. In Proceedings of the 15th NIST-NCSC National Computer Security Conference, pages 554–563, Bultimore, Maryland, USA, October 1992.

[7] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman. Role-Based Access Control Models. IEEE Computer,29(2):38–47, February 1996.

[8] D. Ferraiolo, R. Sandhu, S. Gavrila, R. Kuhn, and R. Chandramouli. Proposed NIST Standard for Role-Based Access Control. ACM Transactions on Information and Systems Security, 4(3):224–274,August 2001.

[9] G. Edjlali, A. Acharya, and V. Chaudhary. History-based Access Control for Mobile Code. In Proceedings of the 5th ACM Conference on Computer and Communication Security (CCS'98), pages 38–48, San Francisco, California, USA, November 1998.

[10] M. Abadi and C. Fournet. Access control based on execution history. In Proceedings of NDSSS'03, pages 107–121, 2003.

[11] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based Encryption for Fine-Grained Access Control of Encrypted Data," Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 89-98, 2006.

[12] R. Sandhu and X. Zhang. Peer-to-Peer Access Control Architecture Using Trusted Computing Technology. In Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05), pages 147–158, Stockholm, Sweeden, June 2005.

[13] J. Bethencourt, A. Sahai and B. Waters, "Cipher text-Policy Attribute-Based Encryption," Proceedings of the IEEE Symposium on Security and Privacy, pp. 321-334, 2007.

[14] K. Yang and X. Jia, "Attribute-based Access Control for Multi-Authority Systems in Cloud Storage," Proceedings of the 32nd IEEE International Conference on Distributed Computing Systems, pp. 536-545, 2012.

[15] T. Ristenpart, E. Tromer, H. Shacham and S. Savage, "Hey, You, Get off my Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 199-212, 2009.

[16] D. Nurmi, R. Wolski, C. Grzegorczyk, S. Soman, L. Youseff and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," Proceedings of the International Symposium on Cluster Computing and the Grid, pp. 124-131, 2009.

[17] B. Shafiq, J. B. D. Joshi, E. Bertino and A. Ghafoor, "Secure Interoperation in a Multi-domain Environment Employing RBAC Policies," IEEE Transactions on

Knowledge and Data Engineering, vol. 17, no. 11, pp. 1557-1577, Nov. 2005.

[18] E. Bertino, P. A. Bonatti and E. Ferrari, "TRBAC: A Temporal Role-based Access Control Model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191-233, August 2001.

[19] J. B. D. Joshi, E. Bertino, U. Latif and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model," IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 1, pp. 4-23, January 2005.

[20] S. Tuecke, "Open Grid Services Infrastructure," pp. 1-86, www.ggf.org/documents/GFD.15.pdf

[21] H. Jin, W. Qiang, X. Shia nd D. Zou, "RB-GACA: An RBAC Based Grid Access Control Architecture," International Journal of Grid and Utility Computing, vol. 1, no. 1, pp. 61-70, May 2005.

[22] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari. 2000. TRBAC: a temporal role-based access control model. In Proceedings of the fifth ACM workshop on Role-based access control (RBAC '00). ACM, New York, NY, USA, 21-30. DOI=10.1145/344287.344298 http://doi.acm.org/10.1145/344287.3442