International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Role Based Encryption with Efficient Access Control in Cloud Storage

G. V. Bandewar[1], R. H. Borhade[2]

[1]Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

[2]Professor, Department of Information Technology, Sinhgad Technical Education Society's SKNCOE, Pune, India

Abstract: ***Cloud computing is a pool of large systems interconnected with each other for scalable data and file storage. With the advantage of this technology cost of computation and storage is reduced incomparably. Cloud can store large amount of data and files virtually so that, it faces many security issues regarding data access ability. Many users of the cloud may lose their control in order to access data from the cloud. To reduce the problem of data access from the cloud many schemes are used to prevent this issue. RBE (Role Based Encryption) is very useful to reduce administration among various users of the cloud. In this paper, a practical RBAC (Role Based Access Control) model is proposed to hold various security features like encryption, role management, role hierarchy, etc. RBAC is the method of coordinating access to computer according to individual roles of the user in an enterprise.***

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

1. Introduction

The idea of cloud computing is depend on the fundamentals like reusability and IT capabilities. Cloud Computing leads to Grid Computing, Distributed Computing, Utility Computing, Autonomic Computing. Highly Scalable Internet based application are hosted on the cloud and tendered as a service to the users of the cloud. Cloud platform is used to design, develop, test the applications offered by the cloud framework. In cloud pay per use services like database management, compute capabilities are granted on demand. Cloud maintains the entire user's data virtually so that, it leads to high attention of data security affair. Data security is a major element in that leads to scrutiny. Like this, the cloud computing has many challenges like data protection, data recovery, management capabilities, compliance restriction. The Cloud computing users do not share physical infrastructure. They rent the usage from the service provider. Sharing resources in a cloud can be improved if any resource remains unnecessary idle. It can reduce the cost significantly and also improves performance. System administrators and software developer centralized on distinct access control to ensure that access will be given only to the authorized user in an organization. RBAC model is emerged for the access control framework [1]. There are three types of access control like user based access control, attribute based access control and role-based access control. A role of a person can display the responsibility and rules for that user. Like, project leader in an organization can lead the project which assigned to the developer in his team. Roles can specify particular duty assigned for that role. With RBAC, role permissions or duties are pretended it makes simple role assignment to the user [3]. Without RBAC it is hard to calculate which permissions are given to which users. There are some basic concepts of RBAC model. These are 1) Role hierarchy- A limited ordered relation rooted among roles. 2) Permission- Shows the duties of authorized users. 3) Access Control- The concept of restricting the access to the resources of the system to the authorized user. 4) Role- Job functions of a particular user that defines the authority of user hold to the role. Some other access models are also present there like MAC and DAC access control framework. RBAC is different from these it can enforce all the policies without any complexity. RBAC can be used to offer security in the large organization with hundreds of users and thousands of permissions. Encryption is a major technique to provide security. Only encryption is not sufficient to provide security. Some access control policies should be there to protect the privacy of data. To protect the privacy of data admin or data owner can employ cryptographic techniques. Role-Based Control Model includes a level of interaction between the users to permission or privileges mapping. The mapping breaks into two steps. That is, user to role and roles to privileges as shown in the fig. 1. The main contribution of the paper is to develop new RBE architecture, implementation of RBE system with the analysis of regarding encryption and decryption time.

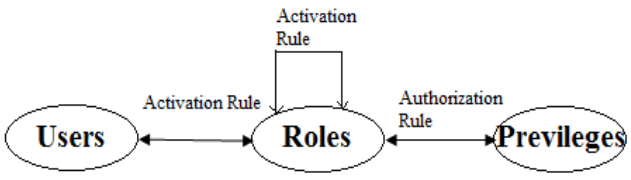

Figure 1: Basic RBAC Model [2]

2. Existing System

A.BGKM (Broadcast group Key management)

In BGKM (Broadcast Group Key Management) the user can decrypt data if and only if their identity attribute satisfy the content provider's policies. The main idea of this scheme is to give some secrets to the users based on their identity attributes and later allow them to derive actual symmetric keys based on their secrets and some public information so that security will be more [4].

B. AB-BGKM (Broad group Key management)
AB_BGKM is the Attribute Based Broad Group Key Management. User can encrypt or decrypt the data based on the attribute of the user. ABAC is used to identify sets of data item to which same access policies are applied and then encrypt each with the same key. It helps in protecting data confidentiality. In GKM (Group Key Management) content publisher delivers symmetric users [5].

C. HBASE (Hierarchical Attribute set based encryption)
HBASE can co-ordinate multiple value assignments for access expiration time to deal with user revocation more efficient than existing schemes. A Hierarchical Attribute-Set-Based Encryption (HASBE) extends cipher-text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. This system achieves greater scalability and flexibility in terms of access control. User revocation can be done more efficiently. ASBE is an extended version of CP-ABE that organizes user attributes into a recursive set structure. ASBE scheme is used for creating hierarchical structure. HASBE is applied for hierarchical user grant; data file creation, file access, user revocation, and file deletion [6].

D. Time Based Proxy Re-encryption
In some cases, data owner should be stay online to distribute proxy re-encryption keys to the users. The delay in issuing the key may results in security risks. To prevent this, the Time Based Proxy Re-encryption is used. It allows user's access rights to expire after pre-specified time period. It includes the concept of time into ABE and PRE. Data is associated with attribute based structure and access time [7].

E. RBCD (Role Based Cascaded delegation)
RBCD (Role Based Cascaded Delegation) system supports simple and efficient cross-domain authority. In this system, delegated privileges are issued to a role of a particular user rather than to that user. In this, role members are responsible to create delegations based on the need of collaboration. In a traditional system, many numbers of signatures required verifying the delegation chain but in RBCD, only one aggregation signature is needed to verify delegation so it will improve performance and efficiency as well. It shows some issues like efficient user revocation and security. Central authority is not available there. So that, it also shows the problem of secure information sharing [8].

F. KP-ABE (Key Policy Attribute Based Encryption)
In this, each cipher-text is knows as encryptor with a set of attributes. And the private key is associated with the type of cipher-text that the key can decrypt. In this, a tree access structure is used in which leaves are associated with attributes. If the attribute is associated with cipher-text then only user can decrypt the cipher-text and if satisfies key access structure.Delegation mechanism is provided in this scheme [9].

G. DACC (Distributed Access Control in Clouds)
This is a new model for data storage and access in the cloud. It avoids storing multiple copies of same data. The main novelty of this system is KDC i.e. Key Distribution centers. Where, KDSs are able to distribute key to the owner or users. Users having same attribute can access the datthea from the cloud. This model results in lower communication, computation and storage overhead [10].

H. MA-FIBE (Multi-Authority Fuzzy Identity Based Encryption)
This scheme focuses on central authority from the multi authority ABE scheme. Central authority can integrate secret keys from other authorities. Purpose of integration is emancipate the user from individual identifiers. This scheme uses key distribution and zero sharing techniques are used to construct MA-FIBE [11].

I. CACH (Content Access Control in Hierarchy)
Independent and dependent key approaches are included in this scheme. To encrypt the data there is no need of encryption key. Users can use their own key with some public parameters. In independent key approach, users must have a copy of that key with which data is encrypted. These are complex techniques [12].

J. Multi-user Searchable Data Encryption Scheme
This model uses keyword encryption scheme. In this each key word is encrypted Additional key pairs are used to encrypt each keyword. This scheme is based on Discrete Logarithms. This model is not distributed to the users. This scheme is built upon proxy encryption [13].

3. New RBE System

There are many access control models are exist but still there is problem of proper access control. RBE scheme with new feature may helps in reducing this drawback.Admin and Role Manager perform different tasks in this system. Admin can upload the data for the user and send the login details and secret key to the appropriate users. Role manager is able to manage the roles of the users. Role manager can change the role of a particular user.

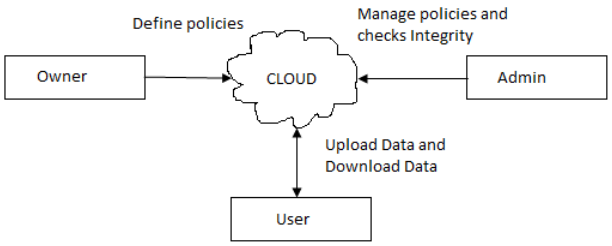

Figure 2: Access Control model

Note: Admin can perform all the tasks of data owner this will helps in improving efficiency.

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

Role Manager is responsible for generating and computing parameters for the users. Role parameters define the position of a user in the role hierarchy.

User can upload the data and they can download the data from the cloud. User can view their profile. Admin will add

the role to user and he can attach policies to the data before uploading file to the cloud so that users with the same policy can access their data from the cloud. User wishes to access their data from the cloud. If users authenticated successfully then their secrets are given to the users. After that user can decrypt their data and can download the data from the cloud using secret key. In this scheme, admin performs various tasks. Public cloud is accessible publically. It also exists outside the environment of the organization

Integrity Check
Many existing RBE systems are able to provide security to the cloud data but still some security issues are found regarding cloud data. It is necessary to provide better authentication to increase access control.

Like this, data privacy is also necessary. In this new RBE scheme, data integrity is verified.

There are four types of RBAC, 1. Symmetric RBAC, flat RBAC, Hierarchical RBAC, constrained RBAC [14].

When user outsources his data to the cloud, while uploading one hash code will be generated and the key to decrypt that data is transferred to the authorized user when admin registers for users. At the user side, when user download the data from the cloud, another hash code will be generated and if both hash codes are same then data is integral. In this case, data is not modified and it is safe. Message will be send to the user if any unauthorized modifications are made. Thus, this new RBE system is more secure than existing systems.

RBE Algorithm:
1. Identify Nodes:
N is main set of each user
N= {A, AU}
Ad - Admin
AU- Authorized User
From this Set of Nodes one Node behaves as server node.

2. Upload File:
AU= {ENC, FN, POL}
FN- File name
ENC - in Encrypted Format
Ad- attaches policies to the files

3. Managing Role:
Ad = {Mk, IDr}
Ad – Manages the role- based upon IDr (Identity of that Role).

4. Sending Encryption Key to authorized user:
AU= {AU1EK, AU2EK, AU3EK….}
Ad – Outsource the encrypted data with attached policies to the cloud.
- Checks role parameters of that user belong with his membership to give access to that user.
- Gives decryption key with the access permission to that user.

Here each Authorized user receives one Encryption Key to Decrypt the File.

5. Authorized User Duty:
AU= {UP, DL, MOD}
Authorized user may Download (DL) upload (UP) or modify (MOD) the file.

The method is simple. In the proposed system, when user uploads the data on the cloud, admin must attach policies regarding users to it, and also he has to encrypt that information before outsourcing to the cloud. AES with TwoFish Algorithm is used for the data encryption and decryption process which is more efficient and requires less time in encryption and decryption than other system. This concept will help in controlling access from the cloud that result in secure searches. New RBE mechanism helps in providing better authenticity. This scheme gives complete focus on access control and data integrity.

4. Implementation

This new RBE is implemented in java and services are presented on tomcat server. It is a servlet container. JDBC-ODBC drivers are used for database connectivity. This system is implemented on Amazon EC2 (Elastic Compute Cloud). Two instances are created on cloud one for EC2 and another is RDS instance which is used for hosting database on the cloud server. Cloud uses SQL database.

5. Result and Discussion

In this section experimental analysis is given. Fig. 3 shows the overall performance of the system. It shows the average time which is required to perform all the tasks. It shows mean time required to encrypt 10 numbers of files from user side. It also shows mean time required to upload and download the files.

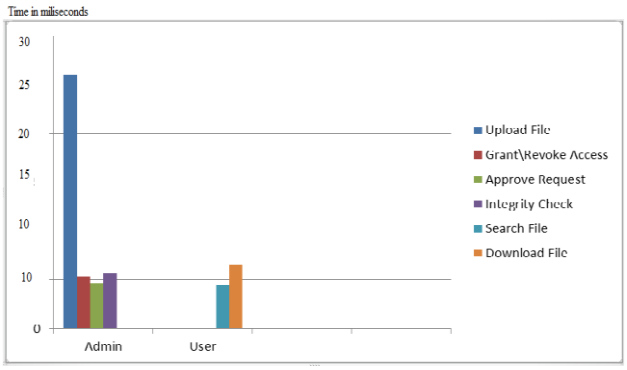

Figure 3: Overall Performance

Fig. 4 shows the time required to encrypt the file before uploading it to the file. It shows comparison between existing and the new system.

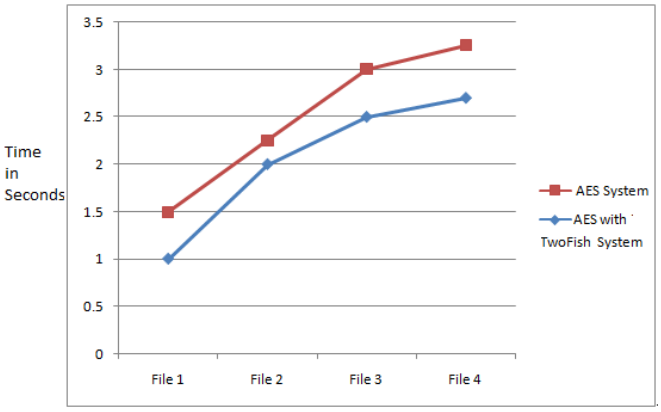

Figure 4: Encryption Time

Fig. 5 shows the time required to Decrypt the file before uploading it to the file. It shows comparison between existing and the new system. This graph shows that encryption time required to encrypt a file before downloading it on the cloud.

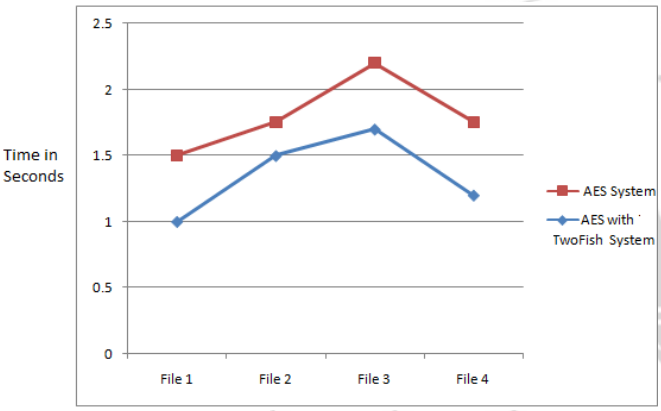

Figure 5: Decryption Time

Table 1 shows the time required to encrypt file. It shows the proper time to encrypt each file. This result shows that existing system require more time than proposed system.

Table 1: Time required for Encryption

Existing RBE Scheme	Proposed Scheme
1.5 ms	1 ms
2.3 ms	2 ms
3 ms	2.5 ms
3.2 ms	2.7 ms

Table 2 shows the time required to decrypt file. It shows the proper time to decrypt each file. This result shows that existing system require more time than proposed system.

Table 2: Time required for Decryption

Existing RBE Scheme	Proposed Scheme
1.5 ms	1 ms
2.8 ms	1.5 ms
2.3 ms	1.7 ms
1.8 ms	1.3 ms

6. Conclusion

In existing systems, some limitations are there like it does not provide data integrity with data privacy. In proposed system, access can be controlled using Role Based Encryption algorithm with the use of access control policies. In existing system, time required to encrypt and decrypt the file is more as compared to proposed system. Thus, data access can be controlled using RBE algorithm.

7. Acknowledgement

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.

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] http://radzserg.com/wp-content/uploads/2015/02/rbac-figure-1.gif
[3] "Role based access control", American National Standard for Information Technology.
[4] M. Nabeel, N. Shang, E. Bertino, "*Privacy Preserving Policy-Based Content Sharing in Public Clouds*", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 11, November 2013.
[5] Punithasurya K, JebaPriya S "Analysis of Different Access Control Mechanism in Cloud", International journal of Applied Information Systems, Vol. 4, September 2012.
[6] Z. Wan, J. Liu, and Robert H. Deng, "*HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing*", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.
[7] Q. Liu, G. Wang, and J. Wu, "Time based proxy reencryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.
[8] R. Tamassia, Fellow, W. H. Winsborough, "Independently Verifiable Decentralized Role-Based Delegation", IEEE Transactions On Systems, Man, And Cybernetics—Part A: Systems And Humans, Vol. 40, No. 6, November 2010.
[9] 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.
[10] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," in TrustCom'11. IEEE,2011.
[11] H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," Inf. Sci., vol. 180, no. 13, pp. 2618–2632, 2010.
[12] H. R. Hassen, A. Bouabdallah, H. Bettarhar, and Y. Challal, "Key management for content access control in hierarchy", Comput Netw, vol. 51, no. pp. 3107-3219, 2007.

[13] C. Dong, G. Russello, and N. Dulay, ―Shared and searchable encrypted data for untrusted servers,‖ Journal of Computer Security, vol. 19, no. 3, pp. 367–397, 2011.
[14] Ravi Sandhu, David Ferraiolo, Richard Kuhn, ―The NIST model for Role Based Access Control: Towards a Unified Standard‖.