VOL. 9, NO. 11, NOVEMBER 2014 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ROLE-BASED ACCESS RIGHTS MODEL FOR CLOUD SYSTEM

P. Shanthi, Bhyravarapu Sri Lakshman, PadavalaPavan Kumar and Panga Siva Reddy
Department of Computer Science and Engineering, SASTRA University, Thanjavur, Tamilnadu, India
E-Mail: shanthip@cse.sastra.edu

ABSTRACT

Due to the abstraction and resourcefulness of the cloud environment, it is emerging to the fore as an answer to the traditional methods. The access rights are used to achieve secure means of data confidentiality and implementation of the business logic. Role based access rights (RBAR) provide a hierarchical model to read and write the data as per authorization and requirement of the implementation logic. The generic models have security drawbacks and are vulnerable to unethical exploits. The proposed model uses broadcast encryption technique and decrypts using respective key. This scheme guarantees, other users/roles are not affected when revoking a user, re-encryption is not needed after user revocation. In this RBAR, the security is improved by limiting the number of users per role, limiting the operations on timely basis and reliability is improved by storing the data for recovery.

Keywords: role-based access rights, cloud environment, security, limiting.

1. INTRODUCTION

Today, security is the primary concern of every field and domain. Role-based access rights enable the individual users of an organization to access the member areas based on their role. When a role is assigned to the user, a user can only access data with what he has been provided. The role-based access rights model is being used for securing the privacy in cloud environment but as the data is large and unlimited in cloud, if any data theft has happened, the loss will be huge and unacceptable.

RBAR is a convincing method for controlling what information system users can utilize, the way they run the program and the modifications they make. Roles are established for various job functions within an organization. Certain operations are allotted to specific roles with some permission restricted to it.

Cloud Computing is the present trending one in the field of development. It is used to build the high end applications with high processing capacity. In cloud we can dynamically change the availability of resources according to the need of application. By using the cloud environment we can reduce the cost for maintaining the application. Cloud is formed by a network of computers, which will take care of all the cores present in the system and makes the user application easier to access.

Cloud computing consists of three types of service models like:

a) **Infrastructure as a Service (IaaS):** This IaaS layer provides the storage and resources to the subscriber based on how much we pay. This layer also deals with the computational power.
b) **Platform as a Service (PaaS):** This PaaS layer provides the components which are required to develop and operate applications over the internet to the subscriber and this layer is one level above the IaaS.
c) **Software as a Service (SaaS):** This SaaS layer makes the same software to be available at once on the cloud for all devices. This layer also allows the subscriber access both resources and application.

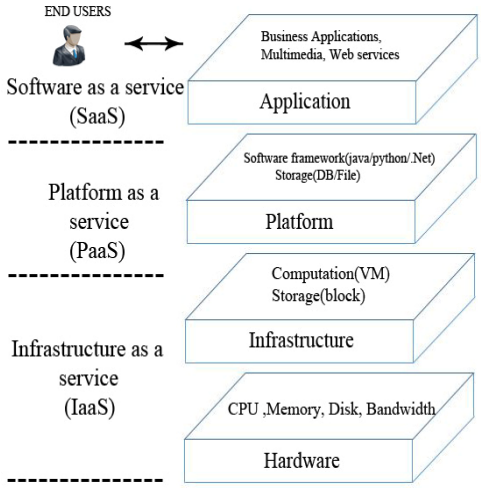

Figure-1. Cloud architecture.

In [1], a public and a private cloud are introduced where data is preserved securely in a public cloud. Users do not know where the data is stored. After the data is uploaded to the cloud, there is a strong ken that users might have lost control over their data. Sensitive information of the organization is stored in the private cloud.

Figure-2. Cloud storage.

The Cryptographic algorithm used is Broadcast Encryption and decryption using the respective key. A Key management block is created. Encrypted data with the key is posted in the key management block. A receiver who has the key same as the keys in the block can take the data. Other receivers can stay calm and wait for the next broadcast. This scheme guarantees other users/roles are not affected when revoking a user, re-encryption is not needed after user revocation.

In this paper, we increased the security, confidentiality and reliability by using "limiting" factors. Access rights are given to the required roles so that the data can be accessed via those rights by the particular role. Only administrator has the rights to limit the limiting factors. Roles accessing the data related to those limiting factors have to access by considering the limit set by administrator; otherwise they are not permitted to access the data.

2. RELATED WORK

An approach to enforce the access rights policies is to change the access rights problem into a problem of key management. In the literature, many hierarchy access control schemes exists which are constructed based on hierarchical key management (HKM) schemes, and enforcing RBAR policies for data storage using HKM schemes. However, several limitations are present for these solutions. For example, for many users and data owners involved, setting up the key infrastructure is very difficult [2, 3].

A different approach for the key management is Hierarchical ID-based Encryption (HIBE). However, in a HIBE scheme, as the growth in the depth of hierarchy increases, the length of identity becomes longer.

Recently, schemes are built directly on RBAC policies [1]. A role-based encryption scheme (RBE) is introduced. But, in this user revocation scheme, all the role related parameters are to be updated. In addition, if different roles are assigned to particular user, the user must possess all the multiple keys. The scheme proposed in the present project overcomes these limitations, and own secret keys are used by each role to update the membership of user so that the secret keys of system are not needed.

Besides RBAR, there are also other access rights models such as Attribute Based Access Control. In this ABAC, based on the attributes, the user will gain the permissions. Systems define collection of all the attributes as the access policies, and users need to prove that these attributes are necessary in order to gain access.

A long history for cryptographic hierarchical structure is present since it is the basic way to manage and organize more users. Many techniques on partial order cryptographic relation hierarchical structure is introduced. Multilevel security problem is solved in [4, 5]. From then, several methods which are efficient have been studied. Logical Key Hierarchy-LKH concept introduced in [6] and [7] have common encryption keys which are arranged into data structure (tree) to accomplish group communication which is secure in the multicast environment.

In Key Policy-ABE technique, accessing the data by users is not in the control of the owner. Respective key to accept or reject the access to specific user is issued by the key-user whom the owner must trust. To rectify this drawback, another scheme is introduced. Here policies and cipher texts are associated with each other, simultaneously user keys and attributes are associated to each other. Therefore, it is stated as the Cipher text Policy-ABE technique. This technique is almost similar to the Role-based access rights and the authors need not provide a crystal correct explanation as to how this scheme can be achieved in the concepts of role-based access and its association with characteristics such as constraints and role hierarchies. Some changes of the CP-ABE technique was proposed in [8, 9] with specifications like constant size solution and cipher text attack secure solution. However, these techniques have drawbacks in achieving revocation in a practical way. Therefore, user's key modification will reflect the keys which make such techniques inefficient in practice.

Another technique was proposed in [10] which consist of hierarchical role-based access rights model. Though, the technique lacks the capacity of user modification, as predecessor roles increases, the size of the cipher text increases.

Other approaches are direct encryption and proxy re-encryption which protect the data privacy in a cloud environment. Here, the users get the encrypted data directly with whom the owners wish that the data should be shared. This is similar to the access control policies in Discretionary Access Control (DAC) model. Hence they are generally used in systems where DAC model is encouraged. As the permissions in such systems are specified either in a flat out structure or in an access matrix, comparison should not be made with present schemes as the access policies specified are different in RBAR model.

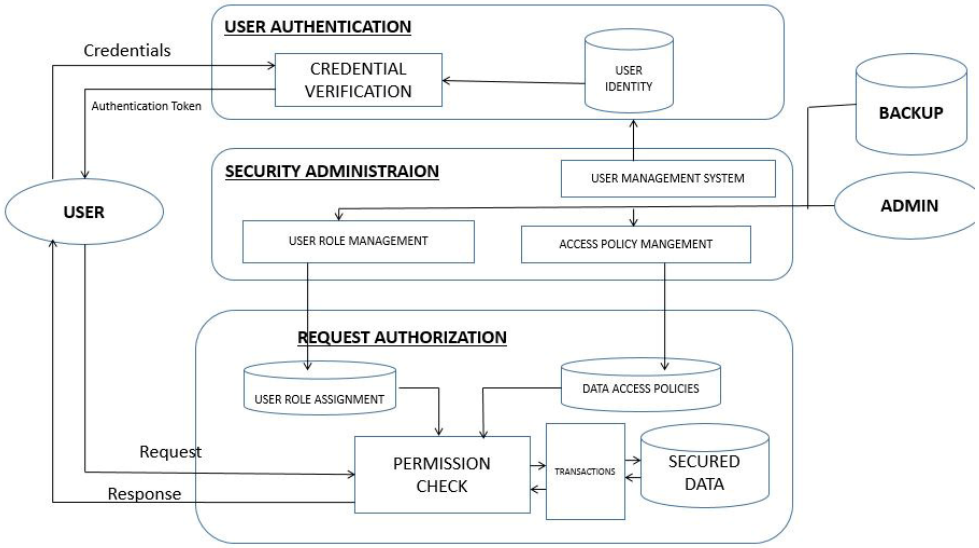

Figure-3. Architecture diagram.

3. ARCHITECTURE

The model consists of users in an organization where each user has login credentials and can access the data with what role he/she has been given. Role hierarchy can be achieved from root node to leaf node in an organization. Each role has certain objectives to accomplish without any irregularities so that all the customers will get used to the functionalities each role provides. Administrator is the sole proprietor for "limiting" restrictions and can assign them dynamically on timely basis. As encryption protects the confidential data, data is secured to the maximum extent. Reliability is achieved through keeping backup in the administrator.

The user credentials are verified in the user authentication block. All the details of user are stored in user identity database and the details entered are checked, if a valid user arrives, he/she is permitted. An authentication token is generated as to which data the user must access. With a given authentication token, the user requests for making a transaction. Then the control is passed to the permission check.

In permission check, first the authentication token is re-verified from the user role assignment database. Secondly, the user is verified for the limiting threshold assigned by the administrator and thirdly, if the threshold is satisfied, then the data access policies are assigned to the user. If the user satisfies the above three conditions, he/she is given rights to perform the transactions.

4. METHODOLOGY

A. Limiting the number of users per role

The module proposed here is used in the User Role Management block in the above architecture diagram. It limits only specific number of users that can access the data with the restriction being held by administrator. Many people will be accessing the cloud for data but if the number of users for a particular role is less, data can be guaranteed to be secure. For example: In a banking application, there can be one user for a manager role, two or more for an assistant manager role and many for a clerk role. If any intruder tries to access the manager's data, he/she cannot, because we have limited the users of manager role to one. Thus security and confidentiality can be maintained.

B. Limiting the operations on timely basis

The module proposed here is used in the Transactions block in the above architecture diagram. Transactions are the most valuable operations that an employee can perform in an organization. Security is the main goal when transactions are performed. So, limiting is applied here with the restriction being held by administrator. As storage of data on cloud is unlimited, there is a possibility of losing all the data when security is breached. So, only limited transactions/operations are permitted to the user for a specific role. For example, if a clerk has performed hundred operations in a day and if any data theft has happened, the entire operations performed by the clerk are worthless. So, by limiting the number of operations (say ten per a day) for a clerk, rules out only those ten operations when a breach has occurred securing the remaining operations.

C. Storing the data for recovery

A backup is added to the admin in the above architecture diagram. It is useful to restore the last modified transactions made by the admin from the local copy stored in the system. In general, the concept of role-based access rights sends the data directly to the cloud computing server; no copy is kept for any kind of backup by the user. A local copy must exist to keep the updates regarding what the administrator changes. For example: Suppose if an administrator unknowingly enters a wrong

security format, it becomes a security threat. So, because of incorrect format, the entire data is lost. If backup is present, then the data which is saved in the local copy can be restored.

5. IMPLEMENTATION

A. System prototype

The above architecture of Role-based access rights model for cloud system is implemented in Asp.net using C#. SQL server is used for persistence of data. For object relational mapping into database, entity framework is used.

Broadcast Encryption is used to hide the real data which is confidential. Data is stored in encrypted format in the database where the roles can see in normal text manner in the view. A key management block is created where all the keys with encrypted data are broadcasted to all the receivers. A receiver (here a role) retrieves only the data if the keys present with him matches the broadcasted keys. This scheme uses a 56 bit key with a 64 bit plain text. A 64 bit cipher text is obtained after all the processing rounds.

B. Experimental evaluation

Performed experiments on five cores: The graph between number of users in the role and cloud operational time is shown below.

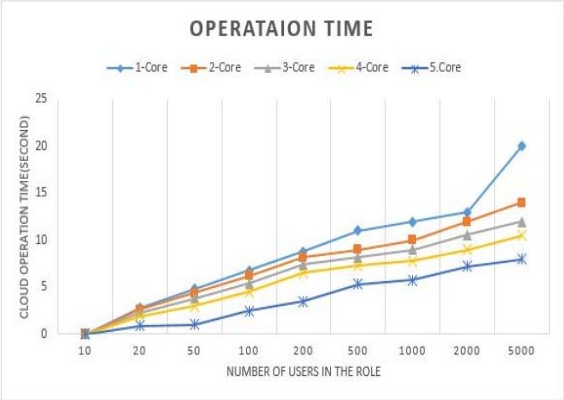

Figure-4. Number of users in the role and cloud operational time.

Data loss is the major concern if any data theft has happened to the transactions. Here, the transaction threshold limit is set to 300. As it is shown below, data loss is very high in existing system whereas in the proposed system it stops at 300th transaction making data loss less and acceptable.

% of data loss if the limiting threshold is 300 transactions

Figure-5.

6. CONCLUSIONS

In this paper, architecture is designed for simultaneous handling of different users ensuring authentication, reliability and security. Security plays a key role in accessing the data in cloud. An RBAR based cloud storage architecture allows an organization to store normal and sensitive data securely in a private cloud. The entire sensitive data present in the cloud is encrypted and decrypted using the broadcast encryption technique. Due to this, the data confidentiality is achieved. It is observed from our experiments that by applying the limiting factors, even if the data theft occurs, loss of data is minimal. Limiting factors achieved security to the paramount extent and reliability is maintained throughout the process.

REFERENCES

[1] Lan Zhou, Vijay Varadharajan and Michael Hitchens. 2013. Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. IEEE transactions on information forensics and security. 8(12).

[2] Abdul Raouf Khan. 2012. Access Control in Cloud Computing Environment. 7(5).

[3] L. Zhou, V. Varadharajan and M. Hitchens. 2011. Enforcing role-based access control for secure data storage in the cloud. Comput. J. 54(13): 1675-1687.

[4] S. Akl and P. Taylor. 1982. Cryptographic solution to a multilevel security problem. In: Advances in Cryptology. New York, NY, USA: Springer-Verlag.

[5] S. Akl and P. Taylor. 1983. Cryptographic solution to a problem of access control in a hierarchy. ACM Trans. Comput. Syst. 1(3).

[6] D. Wallner, E. Harder and R. Agee. 1999. Key management for multicast: Issues and architecture. Nat. Security Agency, Tech. Rep. IETF RFC 2627.

[7] C. Wong, M. Gouda and S. Lam. 1998. Secure group communications using key graphs. In: Proc. ACM SIGCOMM. Vol. 28.

[8] Newport C.C and Cheung L. 2007. Provably Secure CiphertextPolicyAbe.ACMConf. Computer and Communications Security. Alexandria, VA, USA, ACM, New York, USA.

[9] Ibraimi L., Hartel P.H. Tang Q. and Jonker W. 2009. Efficient and Provable Secure Ciphertext-policy Attributebased Encryption Schemes. ISPEC, Xi'an, China, Springer, Berlin.

[10] Zhu Y., Ahn G.-J., Wang H. and Hu H. 2011. Cryptographic Role-based Security Mechanisms Based on Role-key Hierarchy. ASIACCS, Beijing, China, April 13-16, ACM, New York, USA.