



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Authentication and Access Control for Cloud Computing Using RBDAC Mechanism

Varsha D. Mali¹, Prof.Pramod Patil²

Student, Dept. of Computer Networks, NMIET Talegaon Dabhade, Pune, India¹

Asst. Professor, Dept. of Computer Engineering, NMIET Talegaon Dabhade, Pune, India²

ABSTRACT: Role based access controls are suitable for regulating access to resources by known users. However, these Conventional models have often found as inadequate for open and decentralized multi-centric systems. User population is dynamic. All users identity are not known in advance. Cloud computing is becoming one of the emerging and promising field in Information Technology. It provides services to an organization with the ability to scale up or scale down to their service requirements in a networks. Cloud computing services are established and provided by a third party, having the infrastructure. Cloud computing having number of benefits but the most of organizations are worried for accepting it due to security issues as well as challenges having with cloud. Security requirements required for the enterprise level that forces for de- signing models that solves the organizational and distributed aspects of information usage. These models require security policies needed to protect information against unauthorized access and also modification stored in a cloud. To protect the privacy of data it is stored in the cloud, cryptographic role-based access control (RBAC). These schemes have been developed to ensure that data can be accessed by only those who are allowed by access policies. In this project we are proposing trust model to improve the security for stored data in cloud. The proposed trust models provide approach for the data owner and users to determine the individual role. We present a design of a trust-based cloud storage system it shows how the trust models can be integrated into a system that uses cryptographic RBDAC schemes.

KEYWORDS: Role-based access control, Role-based data access control data storage, role-based encryption, architecture, cloud computing.

I. INTRODUCTION

There has been a growing trend to store data in the cloud with the dramatic increase in the amount of digital information such as consumers personal data to larger enterprises. They are wanting to back up databases or store archival data. Cloud data storage can be attractive for users (individuals or enterprises) because it provides unpredictable storage demands, requiring cheap storage tier or a low cost and long-term archive. Service providers can focus more on the design of functions for enhance user experience of their services without worrying about resources to store the growing amount of data by outsourcing clients data to the cloud. Cloud can provide on demand resources so it can help service providers to decrease their maintenance costs. Besides, cloud storage can give a flexible and convenient way for users to access their data from anywhere on any device or gadget. There are distinctive sorts of infrastructures associated with a cloud. A public cloud is a cloud which is made accessible to the general public and also resources are allocated in a pay-as-you-go manner. A private cloud is an internal cloud that is built and operated by a single organization or association. The organization has full control on the private cloud. The private cloud cannot be accessed by external parties. Thus a private cloud is frequently considered to be more secure and trusted.

The proposed trust models contain role inheritance and hierarchy in the evaluation of trustworthiness of roles. A design of a trust-based cloud storage system.shows how the trust models can be integrated into a system and it uses cryptographic RBAC schemes. Many access control models have been proposed throughout the years in the literature. In this fact, role- based data access control (RBDAC) is a well-known access control model which can help to simplify security management especially in large-scale systems. In the RBE scheme proposed in the paper the users management can be decentralized to individual roles, that is, the administrators only manage the roles and the related relationship among them. The roles have the flexibility in specifying the user memberships themselves. The proposed trust models address the missing aspect of trust in cryptographic RBDAC schemes to secure data storage in the cloud

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

and it can provide better protection of stored data than using only cryptographic approaches. The Proposed trust models used for owners and roles in RBDAC systems which are using cryptographic RBDAC schemes to secure stored data.

II. RELATED WORK

In [1] authors used that cryptographic role-based access control (RBAC) schemes have been developed to ensure data can only be accessed by those who are allowed by access policies. In [2] authors highlights challenging issues in data outsourcing are the enforcement of authorization policies and the support of policy updates and solving these issues on the basis the combination of access control with cryptography. For this combines access control and cryptography. In [3] authors proposed a control model which is Role Based Access Control (RBAC), this model provides flexible controls and management by having two mapping, User to Role and Role to Privileges on data. This is the well-known model which can be used for protecting the data in the cloud storage. They have implemented the Role Based Encryption (RBE) scheme which can be implemented with the RBAC model for storing data securely in the cloud system. In [4] authors used a Role-based access control (RBAC) which provides a pliable way for data owners to share and manage their data in cloud. To enforce the access control policies in the cloud, cryptographic RBAC schemes have been developed, which combine cryptographic techniques and access control to protect the privacy of the data in an outsourced environment. A trust model to reason about and improve the security for stored data in cloud storage systems that use cryptographic RBAC schemes. The trust model provides a methods for the owners to determine the trustworthiness of individual roles in the RBAC system. The data owners can use the trust models to decide whether to store their encrypted data in the cloud for a particular role. The proposed trust model takes into account role hierarchy and inheritance in the evaluation of trustworthiness of roles. In [5] proposed the combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. This proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability.

III. PROPOSED SYSTEM

A. RBAC MECHANISM:

Central Repository- In the trust models all the required all interaction histories and trust records identified to roles and users which are stored in a central repository. **Role Behaviour Auditor-** A role behaviour auditor collects the feedbacks for roles from owners and protect the integrity of the feedbacks on roles. **User Behaviour Auditor-** A user behaviour auditor is an entity in trust model. It is used to collect the feedbacks on users' behaviour. **User Behavior Monitor-** A user behavior monitor behave like a proxy server between users and the cloud. It only monitors and forwards the users' requests to access stored data in cloud. **Trust Decision Engine-** The trust decision engine is the entity which evaluates the trust of roles for owners and the trust of users for roles. Channels show flow of system.

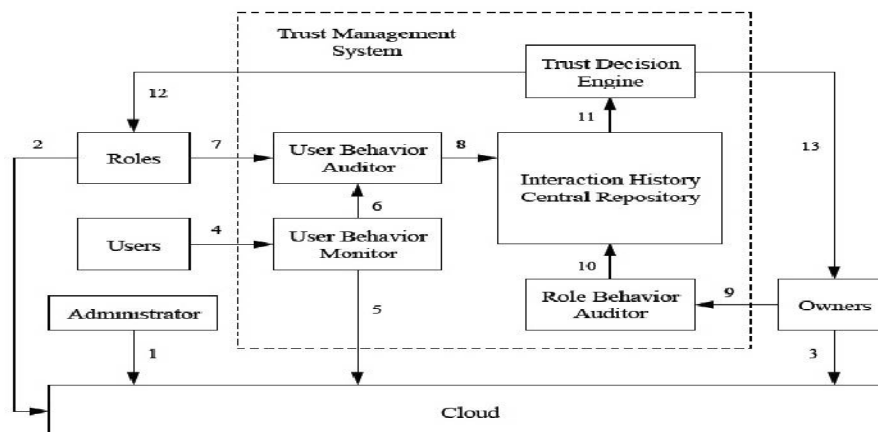


Fig: Architecture for Using Owners Trust Models in a Cryptographic RBAC System

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

B. SYSTEM FLOW DIAGRAM:

The system flow diagram shows two activities one is upload process and another is download process. In the upload process user has to register and then only he can upload his data. This data get encrypted. Next Admin upload this encrypted data on cloud. In download process new user or known user can request for data or file. If file is not present user have to search another file or logout. Now file is present on cloud user request for key. Key is accessed by mobile number or email. After inserting key user get the required file.

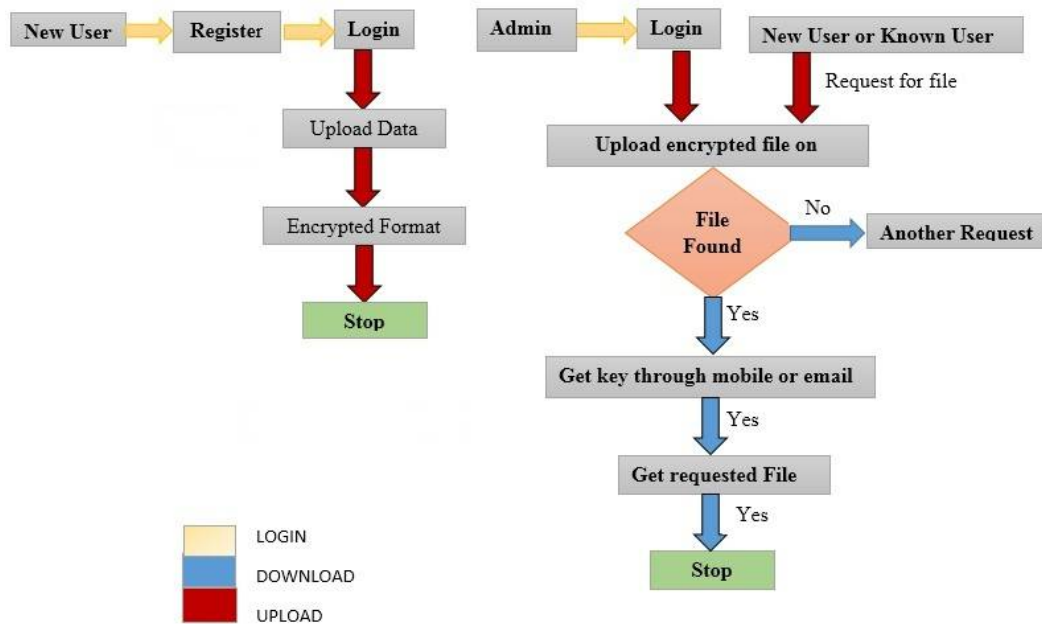


Fig. System Flow Diagram

C. Operations Performed:

The main operations performed are:

1. Registration: Every user must be register with RBDAC system. In Registration process user must fill his personal details of first name, last name, address, mobile no. details etc. Old/Known User directly choose his/her username and password for login in to the system.
2. Upload process:
To upload a file, User use AES Algorithm. Then the file get encrypted. This encrypted file is uploaded to Admin. Admin again encrypt this file by using DES Algorithm. If file is already present then user get a notification of file already exist. And when file not present then file must get upload successfully.
3. Download:
To download a file New or known user have to send request to cloud. Request is forwarded to Admin. Admin generate a key and pass it to requested user. Admin checks for a file, then decrypt it And forwards to the user.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

4. Edit Details:
User has facility to change his/her username and password.
5. Upload details:
Every details of the user gets uploaded to the cloud like his/her first name, last name, username, mobile no. details etc.
6. Request File:
With this operation all valid users can send request for file to the cloud of that particular file.
7. Check File Request:
Admin can also check all file requests sent by the registered user.
8. Send File:
Admin of the file send the particular file to the user who sent request for a file.

D. MATHEMATICAL OPERATION:

1. Let S be a system.

$$S = \{ \dots \}$$

2. Start of the web Server as s

$$S = \{ s, \dots \}$$

Let $s = \{ \text{Start of the web Server: 1. Log in with Server. 2. Deploy the web application on web Server.} \}$

3. Log out system

$$S = \{ s, e, \dots \}$$

Let $e = \{ \text{Log out by user or end of session.} \}$

4. Identify input as X

$$S = \{ s, e, X, \dots \}$$

Let $X = \{ \text{Upload the any file with in cipher text using encryption algorithm.} \}$

5. Identify output as Y

$$S = \{ s, e, X, Y, \dots \}$$

Let $Y = \{ \text{Decrypt this encrypted file to authorized person to access it going to under various security parameters.} \}$

$$X, Y \in U$$

6. Let U be the Set of System.

$$U = \{ DO, UF, CS, CM, SP, DU \}$$

Where DO, UF, CS, CM are the elements of the set.

$DO = \text{Data Owner}$

$UF = \text{Upload file}$

$CS = \text{cloud selection}$

$CM = \text{cloud manager}$

$SP = \text{Specified policy by data owner}$

$DU = \text{Data User}$

E. Algorithm Used:

The following algorithms are used in this role base data access control mechanism.

1. AES
2. DES

These three algorithms are used in this RBDAC mechanism they are described as follows:

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

1. The Advanced Encryption Standard(AES):

For encryption

- a) Substitute bytes
- b) Shift rows
- c) Mix Column
- d) Add Round Key

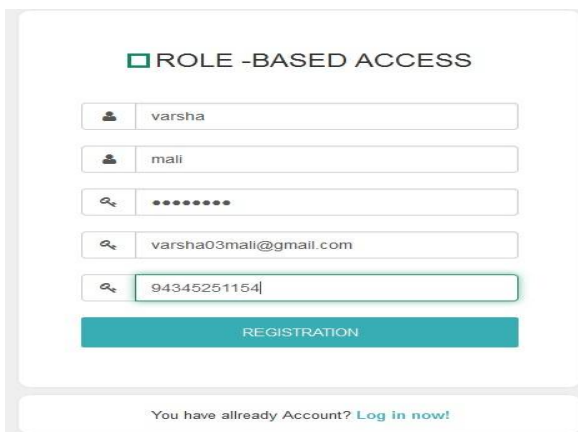
For decryption

- a) Inverse Shift rows
- b) Inverse Substitute bytes
- c) Inverse Add Round Key
- d) Inverse Mix Columns

2. Data Encryption Standard (DES):

DES takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

IV. SIMULATION RESULTS



ROLE -BASED ACCESS

varsha

mali

.....

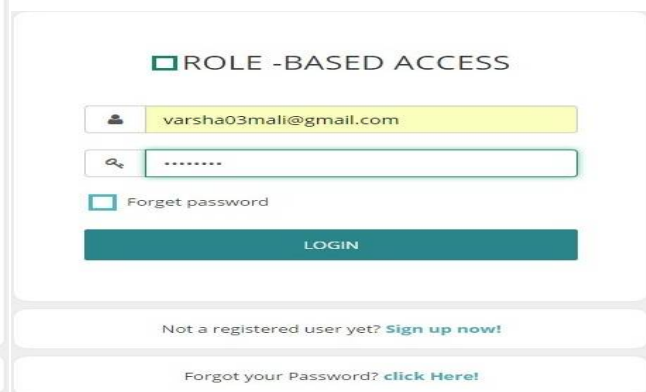
varsha03mali@gmail.com

94345251154

REGISTRATION

You have already Account? [Log in now!](#)

Fig.1.User Register on system



ROLE -BASED ACCESS

varsha03mali@gmail.com

.....

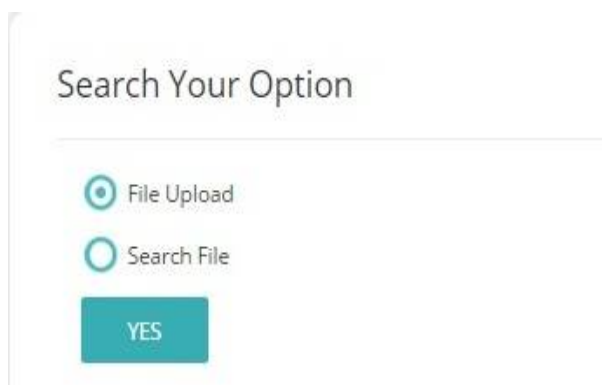
Forget password

LOGIN

Not a registered user yet? [Sign up now!](#)

Forgot your Password? [click Here!](#)

Fig. 2. User Login



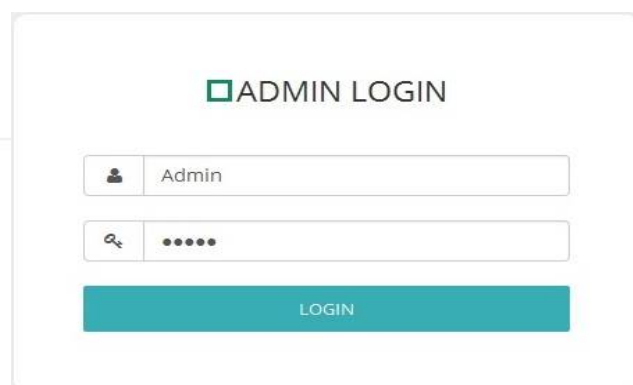
Search Your Option

File Upload

Search File

YES

Fig.3. User Upload File



ADMIN LOGIN

Admin

.....

LOGIN

Fig.4.Admin Login

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

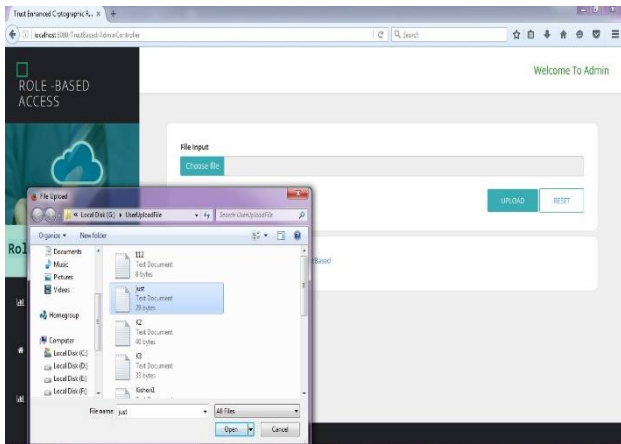


Fig.5. Admin Upload that file in cloud

File Name Are Found

SEND

GET KEY

Fig.6. User Request for file

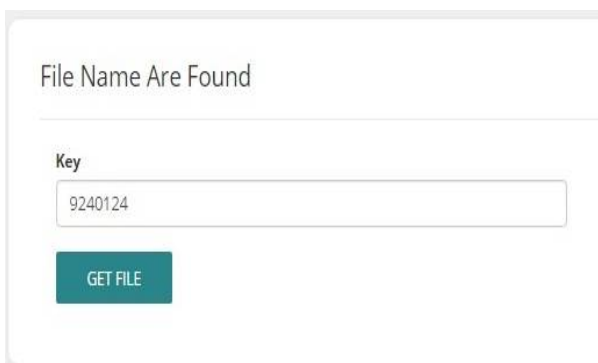


Fig.7. Add key after getting it through mail



Fig .8. Download File

V. CONCLUSION AND FUTURE WORK

Proposed trust models for owners and roles in RBDAC systems which are using cryptographic RBDAC schemes to secure stored data. These trust models contribute owners and roles to become flexible for access policies and cryptographic RBDAC schemes ensure that these policies are enforced in the cloud. The trust models assure the owners and roles to determine the trustworthiness of individual roles and users in the RBDAC system respectively. They allow the valid data owners to use the trust evaluation to decide whether or not to store their encrypted data in the cloud for a particular role. The models also enable the role managers to use the trust evaluation in their decision to grant the membership to a particular user.

REFERENCES

1. LanZhou, Vijay Varadharajan, and Michael Hitchens "Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage" 1556-6013 (c) 2015 IEEE.
2. D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in Proceedings of the 15th NIST-NCSC National Computer Security Conference. NIST, National Computer Security Center, October 10-13 1992, pp. 554 – 563.
3. L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in TrustCom 2013. IEEE, July 2013, pp. 560–569.
4. L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving Secure Role- Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947–1960, 2013.
5. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," in INFOCOM. IEEE, March 15-19 2010, pp. 534–542.
6. M. Toahchoodee, R. Abdunabi, I. Ray, and I. Ray, "A trust-based access control model for pervasive computing applications", in DBSec 2009, ser. LNCS, vol. 5645. Springer, July 12-15 2009, pp. 307-314.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

7. R. S. Sandhu, D. F. Ferraiolo, and D. R. Kuhn, "The NIST model for role-based access control: towards a unified standard", in RBAC00, ACM, 2000, pp. 47-63.
8. H. R. Hassen, A. Bouabdallah, H. Bettahar, and Y. Challal, "Key management for content access control in a hierarchy", Computer Networks, vol. 51, no. 11, pp.3197-3219, 2007.
9. Y. K. Delta, R. Yahalom, B. Klein, and D. T. Beth, "Trust relationships in secure systems-a distributed authentication perspective" in In Proceedings, IEEE Symposium on Research in Security and Privacy, May24-26 1993, pp. 150-164.
10. A. Josang and S. L. Presti, "Analysing the relationship between risk and trust," in iTrust 2004. LNCS. 2004, pp. 135-145.
11. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "A data outsourcing architecture combining cryptography and access control," in Proceedings of CSAW 2007. ACM, November 2007, pp. 63-69.
12. S. D. C. D. Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in VLDB. ACM, September 23-27 2007, pp. 123-134.

BIOGRAPHY

Miss. Varsha D. Mali (P.G.Student) VPM's Nutan Maharashtra Institute Of Engineering And Technology Talegaon Dabhade, Pune, India. She has received B.E. degree in Computer Science & Engineering from M.B.E.S.C.O.E., Ambejogai.

Prof. Pramod Patil Assistant Professor at NMVPM's Nutan Maharashtra Institute Of Engineering And Technology Talegaon Dabhade, Pune, India.