Sec Artillery An enhanced security for content management in cloud

Chitravathi G P[1], Second B. Dr S Nandagopalan[2],
[1] PG Student, Department of Computer Science and Engineering, Bangalore Institute of Technology,Bengaluru.
[2] Professor, H.O.D, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bengaluru.

***Abstract*—.An extensive part of the present organizations relies on cloud for their data storage to handle applications on daily routine where data would be under the control of cloud service provider who offers storage space. The current security solution does not help the data owner or client to have accessing control on their data when it is stored on cloud. Keeping owner of information in mind, we propose a technique called role oriented self-ensured data approach to help organizations to ease access their data where this method controls the data access through roles provided to individual end users within the perimeters of organization by using two ideas, first is mapping users to their roles in company and second is mapping Accessible data to roles where information can be viewed by the end user only if permission is granted to that role as per job profile, position and responsibility by cloud evaluator with the approval from data owner.**

***Index Terms*—Cloud security. Role oriented Security, Data owner, Evaluator.**

I. INTRODUCTION

Security will be the primary concerns for the selection of the cloud processing regarding the client. Clients need to trust the cloud provider for the information security when the information is stored on cloud. The CSP could conceivably get the information or even give it to outsider's vane, however this is normally overseen though lawful or service level agreements (SLA), The current security solution does not help the data owner or client to have control on their own data when it is stored on cloud. The better idea is to secure the contents before the information is uploaded to the cloud and also protect data from cloud service providers even if data may move among clouds. This situation prompts information driven approach where contents is self-secured at whatever point they are situated in cloud. Encryption is the most generally utilized strategy to ensure information in the cloud. Undesired gets is to stayed away from by encrypting the data. However, it makes new issues identified with access management.

In this paper we have focused on the idea of storing the data in a secure way in cloud. The cloud is formed by two or more data centers and is spread geographically. User will be unaware about where the actual data storage and thus this leads to a strong opinion that data would have been lost after uploading into the cloud. Therefore some suitable accessing techniques and policy conditions are required that will restrict or permit data accesses to only those intended end user by the data owner to grant permission to these set of user for their records which is uploaded in cloud.

In Role oriented self-ensured information system , the information is first secluded through double re encoding method before uploading contents into the cloud and information access is given to the end user as per to their allocated role. The mapping of roles to access permissions and users to appropriate roles are taken care. The Evaluator assigns the roles to users in the organization depending on their profile, responsibilities, skills and qualifications. In Role oriented solution, a hierarchy structure depending on roles is considered. Each role can inherit permissions to access contents in cloud from other roles as defined. The Role orient information protection system provides easy management of information by two mappings such as end-user to role and roles to privileges on contents.

II.LITERATURE SURVEY

In current days, to implement access control for securing uploaded cloud data, various plans have been proposed utilizing cryptographic strategies. on the other hand, these methods have several limits. The on high demand required in setting up the key framework can be high, if there are a large number of users and owners are present. In addition, all the remaining users in the same role will be influenced and their keys need to be changed, when a user's permission is revoked, which makes these plans unrealistic. Another approach includes the utilization of the attribute-based encryption. The ABE scheme which involves sets of attributes and private keys are belonging with access frameworks that control which cipher texts where a user is able to decrypt. In Key policyattribute based encryption scheme, the owner of the content does not have the control over information for accessing the data. The data owner trust should be on the key-giver who issues the related keys to grant or disagree access to the appropriate end-users. Another method is CP ABE scheme where the user keys are related with sets of attributes and the cipher's are mapped with the policies. The Role oriented approach is discovered around 1970's and only limited forms of access constraints based on the user's role within an organization. The role based system is straightforward and application specific. Here a role is defined as a set of permissions with subject role activation and role-hierarchies together with subject-object mediation, as well as constraints on user/ role membership and role activation is presented. In Role oriented solution, by updating role related parameters the user revocation is achieved. The issues faced by existing work are ineffectual user revocation, complicated key administration, and Incompetent decryption.

III. PROPOSED METHODOLOGY

A. Data Owner

Since it provides more storage facility than local system, a large portion of vendors move towards cloud for frequently storing their personal data, images, health reports. Data-owners use cloud systems to upload their files etc. In this project work, data owner will encrypt and upload files by using trapdoor generated during encryption. Views all the uploaded files and transactions based on the files uploaded and grant permission to end user to access the files based on their-roles. In this module first, data owner has to get register to the cloud server. He will login to the relating cloud server to which registration was done. The file would be uploaded to the server with the encryption using AES. The data owners would later verify uploaded files and check if it is safe and can view what number of records has been transferred to the comparing cloud-servers.

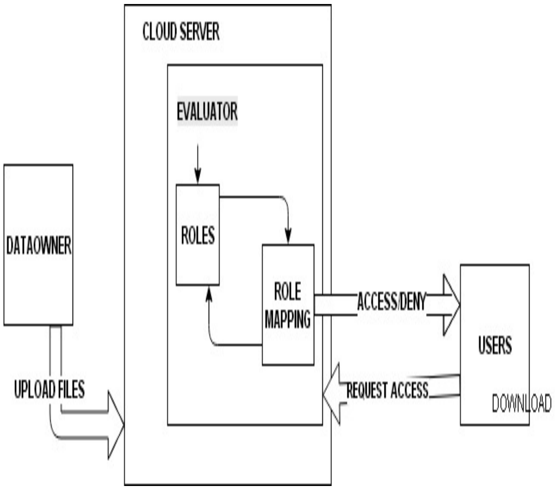


Fig1: Role oriented approach for content management

B. Cloud Server

The cloud server will use encoded format of uploaded files, authorize the users and data owner, view attackers and the check the transactions based on roles and search for transactions. Designed with the set of JSP and html pages, cloud servers are responsible for both allocating the appropriate amount of resources and reserving the time over which required resources are allocated. Access control mechanisms are also defined by CSP.The cloud server used is windows azure which is a Microsoft public cloud platform used for building, deploying, managing application through universal network of datacenters. It consists of queues, blobs and tables as shown below.

C.Evaluator

In this module, the evaluator will offer roles to users, view the same, files with encrypted attributes and transactions based on roles. The login and authorization for both data owner and end user are provided by it. Evaluators list the numbers of users in cloud-services also can view the attackers and the no of time attacked. He is responsible for authorizing users and grant permission for applying rules.

D. End User

In this module, the user will register to access contents in cloud. Based on roles, he would be granted permission to search for download files. Search for the file will be based on the content keyword and request for it and download with the secret key for the corresponding file from cloud and download them.

E.Roles

It is a representation of access control at high level. Among individual end users and permissions many to many relationship exists. Role includes a mapping between a user and a subset of each role that are allocated to users. The hierarchy of roles is used to give the role to end-users in the system.

F. Role Mapping

Users are classified according to their roles. The cloud evaluator provides access of files or contents to be downloaded or uploaded by the end user depending on the roles granted to him.

IV.ARCHITECTURE

The above figuredemonstrates a framework with design is proposed with criteria of how access to ensure information is accomplished for the utilization of model inside CSP's. This incorporates four models such as data owner, cloud service provider, Evaluator and end user portals. The client or the data-owner approaches cloud for storing his/her information such as health reports, email, documents etc by registering and logging in to the cloud-system since it provides more storage and security than local system.

Before storing user data like files, into the cloud, the secluded wrap up is created by data owner which contain the encrypted objects, conditions for accessibility of files together with corresponding reencoded keys. While uploading files or contents to cloud, the data-owner randomly generates the trapdoor and secret key using the encrypt function.

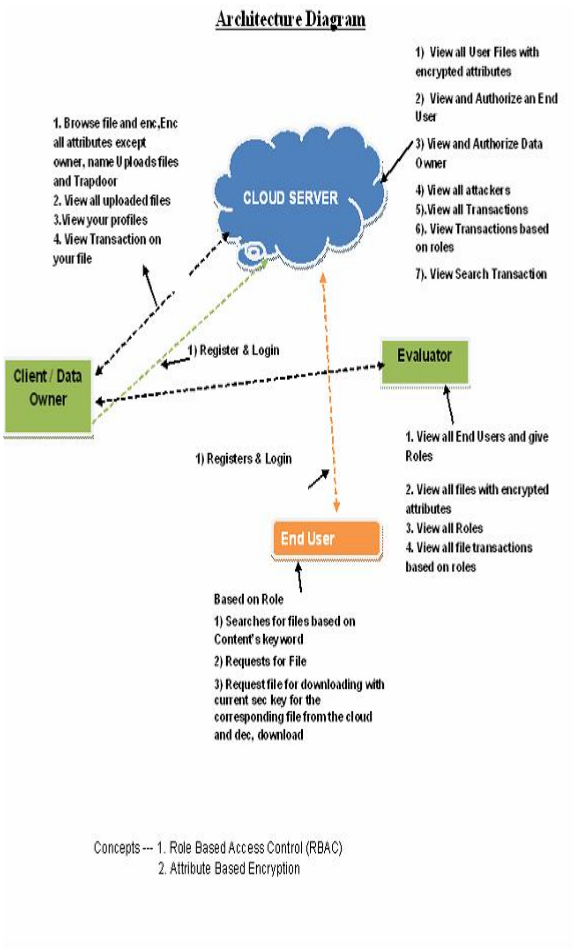

Architecture Diagram
1) View all User Files with encrypted attributes
2) View and Authorize an End User
3) View and Authorize Data Owner
4) View all attackers
5).View all Transactions
6). View Transactions based on roles
7). View Search Transaction
1. Browse file and enc,Enc all attributes except owner, name Uploads files and Trapdoor
2. View all uploaded files
3.View your profiles
4. View Transaction on your file
CLOUD SERVER
1) Register & Login
Client / Data Owner
Evaluator
1) Registers & Login
1. View all End Users and give Roles
2. View all files with encrypted attributes
3. View all Roles
4. View all file transactions based on roles
End User
Based on Role
1) Searches for files based on Content's keyword
2) Requests for File
3) Request file for downloading with current sec key for the corresponding file from the cloud and dec, download
Concepts --- 1. Role Based Access Control (RBAC)
2. Attribute Based Encryption

Fig 2: System architecture

For role based access control the preconditions are characterized and directly data owner would map it directly. Depending on the roles, the right to use for the files is given. For every auth-rule reencryption keys are generated. Those artifacts are encrypted using the AES encryption algorithm to ensure privacy, security and then outsource onto cloud hence providing data-centric-security to client-data. The data owners are responsible for browsing the files and encrypt all attributes such as name, type and content except owner names and generates trapdoor during uploading the files.

The data owner is accompanied with the task of uploading files and generating trapdoor, viewing profiles and viewing transaction based on roles. The cloud server is used for data storage. Client must login with unique login id and password to verify the uploaded files in the data center and authorize data owners and end users, also responsible for viewing user files but in encrypted manner and viewing all types of transactions.

Meanwhile Evaluator which ensures data security based on roles is responsible for granting roles to the end user, viewing all types of transaction based on roles, granting to the end-users and verifying related transactions, encrypted attributes thus ensuring role based access control solution. Based on roles granted to the end-user, the final user searches the file relating to the content of keyword. Request for the files is granted depending on the roles, requested file with secret key would be downloaded by the user.

V.ALGORITHM

In Role oriented approach, following steps are used:

1) **Setup:** The input is public parameter p for this algorithm which produces master secret key (mk) and public key (pk).

2) **Create Data owner:** the data owner should be registered with the cloud before uploading the content.

3) **Upload file:** the files should be encrypted twice before uploading to cloud using master secret key.

4) **Encrypt:** Encryption is done by the owner of the data. This algorithm takes role_id, public_key and point on the elliptic curve as an input and generates cipher text of the message. The details of the encrypted data are stored on the cloud.

5) **Generate Role:** Role with distinctiveness arrangement is added. The Evaluator executes this part by creating role. A role hierarchical set is preserved where all the roles are viewed and stored in the framework by utilizing public parameter.

6)**AddEnd user**: Cloud server administrator and evaluator execute this pseudo code in which Evaluator gives Role to user and cloud service provider provides authentication. The list of role users is updated in cloud. .

7)**Authorization**: authorize both data owner and end user before accessing to contents of clouds.

8)**Grant permission:** the data owner and cloud service provider both grant permission to end user for accessing files

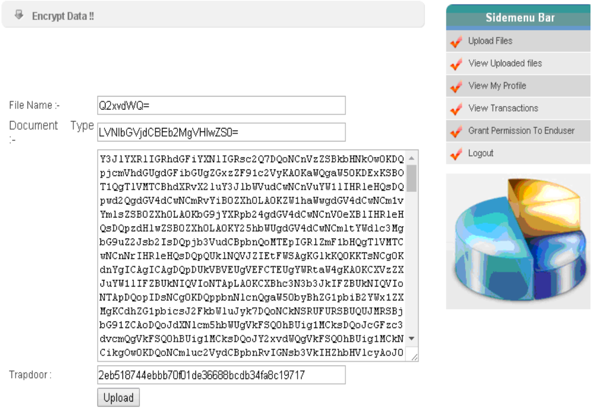
9)**Download file**: With the enough accessing permission on specified roles of end users, the file can be downloaded.

10)**Decrypt**: Users who possess access according to their role this algorithm is executed.

VI. EXPERIMENTAL RESULTS

The Testing results of the Proposed Methodology is Very efficient, it can enable content or file access in an encrypted form with an secluded manner and based on roles granted and authorized by cloud service provider and evaluator with the permission from the data owner.

A. Experimental setup:



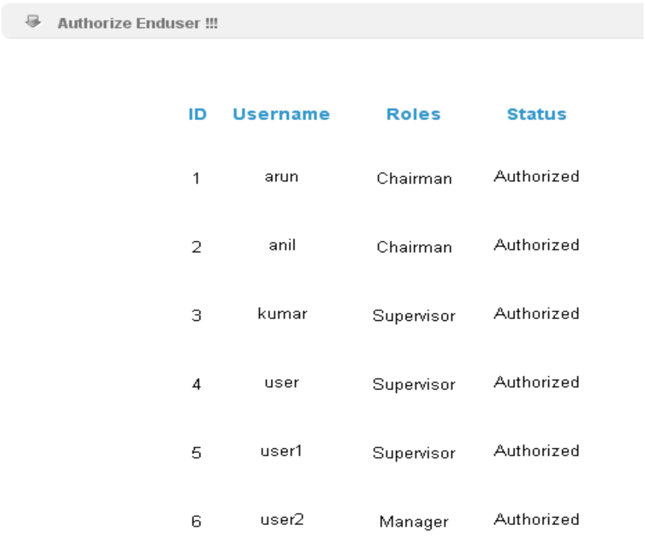
File Name :- Q2xvdWQ=

Document Type :- LVNlbGVjdCBEb2MgVHlwZS0=

Y3J1YXR1IGRhdGFiYXN1IGRsc2Q7DQoNCnVzZSBkbHNkOw0KDQ
pjcmVhdGUgdGFibGUgZGxzZF91c2VyKA0KaWQgaW50KDExKSBO
T1QgT1VMTCBhdXRvX2luY3J1bWVudCwNCnVuYW11IHR1eHQsDQ
pwd2QgdGV4dCwNCmRvYiB0ZXh0LA0KZW1haWwgdGV4dCwNCm1v
YmlsZSB0ZXh0LA0KbG9jYXRpb24gdGV4dCwNCnV0eXB1IHR1eH
QsDQpzdH1wZSB0ZXh0LA0KY25hbWUgdGV4dCwNCm1tYWdlc3Mg
bG9uZ2Jsb2IsDQpjb3VudCBpbnQoMTEpIGR1ZmF1bHQgT1VMTC
wNCnNrIHR1eHQsDQpQUk1NQVJZIEtFWSAgKG1kKQ0KKTsNCg0K
dnYgICAgICAgDQpDUkVBVEUgVEFCTEUgYWRtaW4gKA0KCXVzZX
JuYW11IFZBUkNIQVIoNTApLA0KCXBhc3N3b3JkIFZBUkNIQVIo
NTApDQopIDsNCg0KDQppbnNlcnQgaW50byBhZG1pbiB2YWx1ZX
MgKCdhZG1pbicsJ2FkbWluJyk7DQoNCkNSRUFURSBUQUJMRSBj
bG91ZCAoDQoJdXNlcm5hbWUgVkFSQ0hBUig1MCksDQoJcGFzc3
dvcmQgVkFSQ0hBUig1MCksDQoJY2xvdWQgVkFSQ0hBUig1MCkN
CikgOw0KDQoNCmluc2VydCBpbnRvIGNsb3VkIHZhbHVlcyAoJ0

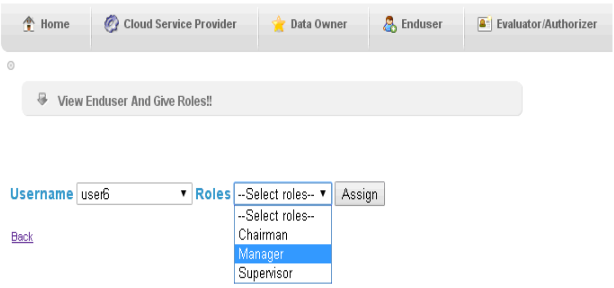
Trapdoor : 2eb518744ebbb70f01de36688bcdb34fa8c19717

Fig3: Data owner content Encryption before Uploading to cloud



ID	Username	Roles	Status
1	arun	Chairman	Authorized
2	anil	Chairman	Authorized
3	kumar	Supervisor	Authorized
4	user	Supervisor	Authorized
5	user1	Supervisor	Authorized
6	user2	Manager	Authorized

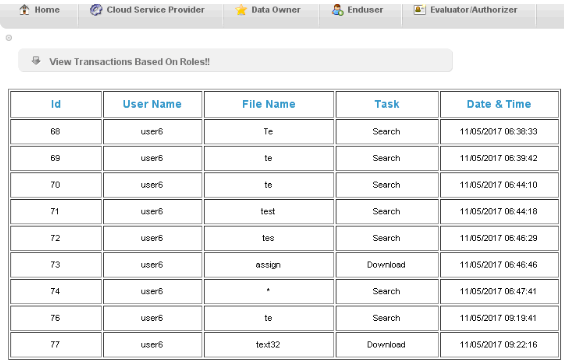
Fig4:Roles authorization



Username user6 Roles --Select roles--

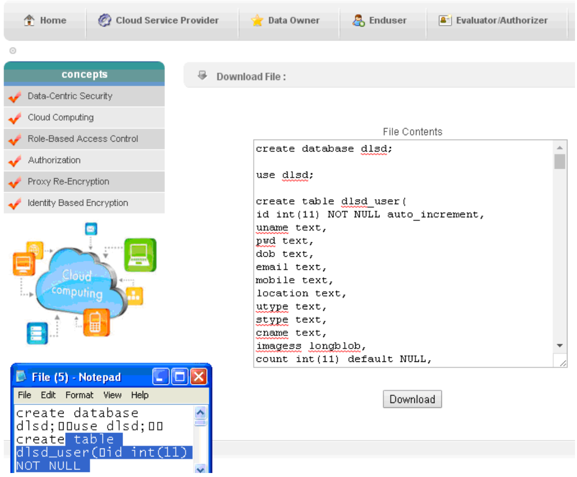
--Select roles--
Chairman
Manager
Supervisor

Fig5: Evaluator assigning roles



Id	User Name	File Name	Task	Date & Time
68	user6	Te	Search	11/05/2017 06:38:33
69	user6	te	Search	11/05/2017 06:39:42
70	user6	te	Search	11/05/2017 06:44:10
71	user6	test	Search	11/05/2017 06:44:18
72	user6	tes	Search	11/05/2017 06:46:29
73	user6	assign	Download	11/05/2017 06:46:46
74	user6	*	Search	11/05/2017 06:47:41
76	user6	te	Search	11/05/2017 09:19:41
77	user6	text32	Download	11/05/2017 09:22:16

Fig 6: View transaction based on roles



```
create database dlsd;

use dlsd;

create table dlsd_user(
id int(11) NOT NULL auto_increment,
uname text,
pwd text,
dob text,
email text,
mobile text,
location text,
utype text,
stype text,
cname text,
imagess longblob,
count int(11) default NULL,
```

```
create database
dlsd;□□use dlsd;□□
create table
dlsd_user(□id int(11)
NOT NULL
```

Fig7: Download file only based on roles granted

VII.CONCLUSION

This proposed work defines focusing on the security in cloud by utilizing the idea of role oriented access control solution and focus on safely storing the information through encryption before uploading data into the cloud using the evaluator and rule based approach. It provides an enriched expressiveness using advanced cryptographic techniques. Here CSP would be unable to access the information and release to unauthorized third parties though access control computation is given and thus providing data centric authorization solution for secured data protection in cloud.

REFERENCES

[1] Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing v3.0,” CSA, Tech. Rep., 2003.

[2] Y. Zhang, J. Chen, R. Du, L. Deng, Y. Xiang, and Q. Zhou, “Feacs: A flexible and efficient access control scheme for cloud computing,” in Trust, Security and Privacy in Computing and Communications, 2014 IEEE 13th International Conference on, Sept 2014, pp. 310–319.

[3] B. Waters, “Cipher text-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in Public Key Cryptography - PKC 2011, 2011, vol. 6571, pp. 53–70.

[4] B. B and V. P, “Extensive survey on usage of attribute based encryption in cloud,” Journal of Emerging Technologies in Web Intelligence, vol. 6, no. 3, 2014.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proceedings of the 13th ACM Conference on Computer and Communications Security, ser. CCS ’06, New York, NY, USA, 2006, pp. 89–98.

[6] InterNational Committee for Information Technology Standards, “INCITS 494-2012 - information technology - role based access control - policy enhanced,” INCITS, Standard, Jul. 2012.

[7] E. Coyne and T. R. Weil, “Abac and rbac: Scalable, flexible, and auditable access management,” IT Professional, vol. 15, no. 3, pp. 14–16, 2013.

[8] Empower ID, “Best practices in enterprise authorization: The RBAC/ABAC hybrid approach,” Empower ID, White paper, 2013.