A Survey of An Attribute Based Encryption and Access Control Model in Cloud Storage Environment

[1]Akshada Yevatkar, [2]Dr. S. Y. Amdani
[1]PG student, [2]Professor ,
[1] Department of CSE,
Babasaheb Naik College of Engg. Pusad

Abstract : ***For big industries and academia as well, cloud is becoming an essential tool for data repository maintenance. Cloud computing is a set of different types of hardware and software activities that work collectively to deliver many aspects of computing to the end user as an online services. It provides on demand scalable and cost effective services for storing documents. However with all of these services it comes up with number of challenges associated with utilizing the cloud securely. Achieving unbreakable document or outsourced data security is again a very important issue to consider. To provide security to the outsourced documents, Attribute based encryption is an excellent solution. In this paper, we are going to do analysis main attribute based encryption encryption scheme and its related access control models available for handling data under various scenarios of the cloud storage environment.***

IndexTerms - Attribute Based Encryption, Access Control, Bilinear Map, Diffie Hellman Assumption

---

I. INTRODUCTION

Cloud Computing is a usage based service where you can obtain various network resources such as networked storage space. The current scenario is, the data owner upload his/her data to the cloud with an access policy associated with it. But in this case, anyone who satisfy that particular policy will be able to acquire the data. To overcome this, cryptography have been suggested. Encryption is the way to secure data on the untrusted cloud. But only cryptography is not sufficient to solve this problem because in case of key leakage, the documents can be hacked by the attackers . Also when the ciphertext is needed to be share with others and the cloud has no rights to decrypt the data then the problem becomes more challenging. The excellent solution for this problem is an Attribute Based Encryption. ABE[1] provides an entirely new vision of encrypting data. Instead of encrypting to individual users, in an ABE system, one can employ any access policy into the the ciphertext itself. These policies can enforce either role-based or content or attribute based access controls [6]. Thus, data access is self-enforcing through the cryptography.

This paper summarizes ABE classified schemes mentioned in mainstream papers and analyzes each scheme with algorithm. Attribute Based Encryption related mathematical fundamentals such as bilinear map and the security assumptions of ABE are discussed in Section 2. An overview of ABE, classification of ABE scheme and Access Control models/techniques is given in Section 3. Proposed Work is given in Section 4.

II. BACKGROUND

In this Section we discuss the mathematical terms in Attribute Based Encryption (ABE) that increases the security of ABE scheme.

A. Bilinear Maps

Shamir invented IBE system in1985 [1],but the key generation of the IBE system remained a challenging Problem. Significant approaches such as RSA, Diffie Hellman [4] were failed to transform into IBE. Compared with the earlier approaches, bilinear map is efficient at key generation secure [2]. Bilinear maps are the tool of pairing based cryptography. It is a function that combines element of two groups of same order to yield an elements of third group and establish a relationship between cryptographic groups.

Definition of a Bilinear Map –

> Let G1, G2, and Gt be cyclic groups of the same order *A bilinear map from* $G_1 \times G_2$ *to* G_t *is a function* $e : G_1 \times G_2 \rightarrow G_t$ *such that for all* $u \in G_1, v \in G_2,$ $a, b \in Z, e(u^a, v^b) = e(u, v)^{ab}$.

Bilinear maps are called pairings because they associate pairs of elements from G_1 and G_2 with elements in G_t . This definition admits degenerate maps which map everything to the identity of G_t .

Let G and GT be cyclic groups with the same large prime order q. A bilinear map *e* is defined as: $e: G_1 \times G_2 \rightarrow G_T$.
Following are the properties, Bilinear Maps should posses –

1. Bilinearity: $(g^a_1, g^b_2) = e(g_1, g_2)^{ab}$. g_1 and g_2 are the generators of G_1 and G_2 respectively, a, b ∈ Z. Whereas G_1 and G_2 are the source group, and GT is the target group.
2. Computability:The bilinear map *e* is efficiently computable for any pairs given by $G_1 \times G_2$.
3. Non-degeneracy: *e* (g1, g2) ≠1. It means the map does not send all pairs in $G_1 \times G_2$ to the identity in G_T [7]. Bilinear maps that fulfills this properties are also known as admissible bilinear maps.

B. Security Assumptions

Bilinear map is the mainstream solution for identity based encryption and attribute based encryption. The security of bilinear map solution is based on Computational Diffie Hellman assumption. Boneh[] et.al proved that for finite order groups, the security of bilinear map is strong if it holds computational diffie hellman(CDH) assumptions in it.

The formal definition of CDH is as follows:
For any cyclic group G with order q and a randomly chosen generator g, given tuple
{g; g^a; g^b) | a, b ∈ Z}, computing the value of g^{ab} is called the computational Diffie-Hellman problem (CDH). However computing g^{ab} is hard to control or deal with, because since the discrete logarithm of value base a generator is complex.

- Bilinear Diffie Hellman(BDCH) is an extended form of diffie hellman assumption on which, security of value generated by bilinear map is based. In BDCH given that g, g^a, g^b, g^c, and we have to compute $e(g, g)^{abc}$, where *e* is the bilinear map function and g is a group of same order. Fuzzy IBE scheme [3] and KP-ABE [9] are proven to be secure under the Decisional Bilinear Diffie - Hellman (DBDH) [4] assumption. DBDH assumption distinguishes
g, g^a, g^b, g^c, $e(g, g)^{abc}$ from g, g^a, g^b, g^c, $e(g, g)^z$.

These mathematical terms are foundation of any Attribute based encryption scheme that are useful in setup of system environment and mostly common in every ABE system.

III. SURVEY

This survey discusses the overview of ABE scheme, classification of ABE schemes and traditional Access Control models in cloud storage environment.

1.1 ABE Overview

Amit Sahai, Brent Waters in 2005 [5] first proposed the notion of ABE. In ABE, a set of descriptive attributes is used as an identity to generate secrete key as well as the access structure that performs access control.
The basic model derived from Fuzzy-IBE, which contains Setup, Key Generation, encrypt, Decrypt algorithm.Almost all cryptographic system that uses ABE are consist of atleast these four modules.
The system environment can be set up as follows:
Let security parameter Ƙ determine the size of the bilinear source group.
ABE consist of four algorithms i.e setup, key generation, Encrypt and Decrypt.

Algorithm 1:

- *setup(Ƙ) →PK,MK*

setup the environment for bilinear mapping, taking *Ƙ* as an input parameter and returns public key and master key as output. Where K is a size of an attribute set.

- KeyGen(MK, τ) → *SK*

For threshold access policy, key generation consist of abstractions of a user's attributes set S. and the KeyGen function will take MK and the access tree τ as input and generate a secret key SK for the user.

- Encrypt(M,S,PK,) → CT

The encrypt algorithm takes a plaintext M as well as a set of expected attributes S' as input and outputs the ciphertext CT.

- Decrypt(CT,SK) → M

The decyption algorithm will take the user's SK and ciphertext CT as input and returns the message M or NULL if access is denied.

To enhance the security of system, there is need of adding atleast one parameter or algorithm in the above scheme, so that system will be more complex, thereby increase the performance.
Limitations of ABE are as follows:
(1) Different categories of users create a computational overhead
(2) Lack of an express ability in the sense of a threshold value.

.

1.2 Classification of ABE

ABE schemes are broadly classified as follows.

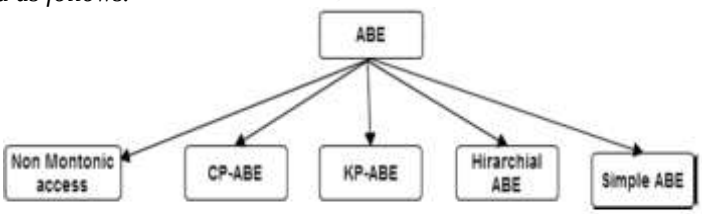

Fig.1: Classification of ABE schemes

1.2.1 Key-Policy ABE

KP-ABE was proposed by Vipul Goyal, Omkant Pandey et.al[7], it is a variation in attribute based encryption. The decisional bilinear DiffieHellman assumption was used for the technique and supports for fine grained access control. The KP-ABE consist of four algorithms, described as follows –

Algorithm 2 :

1. Setup(k) → PK,MK
2. Encryption(M,S,PK) → E
3. Key Generation(A,MK) → D
4. Decryption(E,S,D) → M *if* S ∈ A *else* ⊥

k=security parameter	A=Access Structure
PK=public parameter	S=attribute set
E=ciphertext	MK=master key
D=decryption key	M=message(plaintext)

Initially security parameters are setup to encrypt the message M and descriptive attribute S using PK to generate Ciphertext (E), as shown in Algorithm 2. In KP-ABE decryption[18], a key is embedded with an access structure. The decryption of the ciphetext is only possible if the attributes of the E satisfy the access structure of the user's secret key.The drawback of kp-abe scheme is that the encrypted data cannot choose who can decrypt the message or data shared.

1.2.2 Ciphertext Policy ABE (CP-ABE)

The CP-ABE scheme is another variant of ABE proposed by J.Bethencourt, Amit Sahai, Brent Water in 2007 [2]. In this scheme, a user is able to decrypt a ciphertext, only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE enables the encryptor to choose the access policy to decide who is authorized to acquire the data. and let the ciphertext i.e encrypted data in the access structure decides which key can recover the data. An ciphertext-policy attribute based encryption scheme consists of four fundamental algorithms and one optional algorithm: Setup, Encrypt, KeyGen, Decrypt and Delegate.

Algorithm 2 :

1. Setup(k) → PK,MK
2. Encrypt(M,S,A) → E
3. Key Generation(A,MK) → SK
4. Decrypt(PK,E,SK) → M
5. Delegate(SK, Ã)

k=security parameter	A=Access Structure
PK=public parameter	S=attribute set
E=ciphertext	MK=master key
D=decryption key	M=message(plaintext)
Ã=set of S	SK=secrete key

The setup algorithm take the implicit security parameter. It outputs the public parameters PK and a master key MK. Encryption takes as input the public parameters PK, a message M, and an access structure A over the universe of attributes and returns ciphertext. here we assume that the ciphertext implicitly contains A. generated ciphertext able to find a user that possesses a
set of attributes that satises the access structure. The key generation algorithm takes as input the master key MK and a set of attributes S that describe the key and returns a psecrete key SK.For Decryption, If the set S of attributes satis_es the access structure A then the algorithm will decrypt the ciphertext and return a message M. The delegate algorithm takes as input a secret key SK for some set of attributes S and a set Ã is subset of S. It output a secret key SK for the set of attributes Ã, It depends on encryptor whether to use this algorithm or not. It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment.

3.2.3 ABE with Non-Monotonic Access

Ostrovsky et al.[9] proposed an attribute-based encryption with non-monotonicaccess structure in 2007. Previously proposed ABE schemes were limited to expressing monotone access structure and there is no possible way to declare negative attributes in the access structure.

Algorithm 3 :

1. *Setup (d).*
2. *Encrypt (M, γ,PK).*
3. *Key Generation (˜A,MK,PK)*
4. *Decrypt (CT;D):*

d=number of attributes γ=set of attributes

PK=public parameter ˜*A*=Access structure
MK=master key CT=ciphertext
D=private key

Setup (d). A parameter d specifies how many attributes every ciphertext has.
Encryption (M, γ,PK). To encrypt a message M ∈ GT under a set of d attributes $\gamma \subset Z^*$ p, choose a random value s ∈ Zp and output the ciphertex CT.
Key Generation (˜A,MK,PK) outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that ciphertext satisfy the access structure ˜A.
Decrypt (CT,D): Input the encrypted data *CT* and private key *D*, if the access structure is satisfied it generate the original message M.

3.2.4 Hierarchical ABE

Hierarchical ABE is a composition of the features of HIBE and CP-ABE. HABE model was proposed by Z. Wan et.al[10], model given below consists of a root master(RM) , the third trusted party (TTP), multiple domain masters (DMs) in which the top-level DMs correspond to multiple enterprise users.

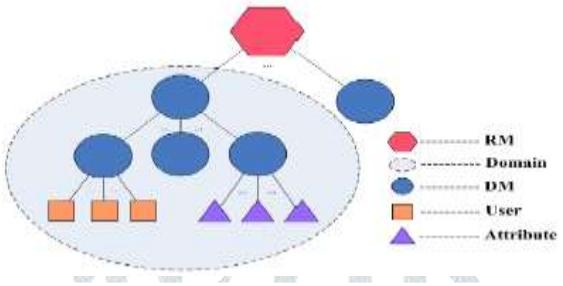

Fig.2: HABE model

HABE consists of five algorithms as –

Algorithm 4

1. Setup (K)→(params,MK_0)
2. CreateDM(params,MK_i, PK_i+1) → (MK_i+1)
3. CreateUser(params,MK_i,PK_u,PK_a)→($SK_{i,u}$,$SK_{i,u}$,a)
4. Encrypt(params; f ;A; {PKa|a E A})→(CT)
5. Decrypt(params,CT,$SK_{i,u}$,{SK_i,u,a|a∈CC_j})→(f)

K= security parameter Params=system parameters
MK_0=root master key PK=public parameters
SK=secrete key CC_j=jth conjunctive clause

Setup -The RM first picks $mk_0 \in Zq$, and then select groups G1 and G2 of order *q*, a bilinear map $e : G1 \times G1 \rightarrow G2$, two random oracles $H1: \{0; 1\}^* \rightarrow G1$ and $H2: G2 \rightarrow \{0, 1\}^n$ for some *n*, and a random generator $P_0 \in G1$. Let $Q_0 = mk_0 P_0 \in G1$. The system parameters *params* will be publicly available, while $MK_0 = (mk0)$ will be kept secret.
CreateDM takes params and master key and generates Domain master or Root master. CreateUser creates user if it is eligible for, which he has administered.
Encrypt algorithm,takes a file f, a DNF access Control policy A, and public keys of all attributes in A, as inputs, and outputs a ciphertext CT.
Decrypt algorithm A user, whose attributes satisfy the j-th conjunctive clause CCj, takes params, the ciphertext, the user identity secret key, and the user attribute secret keys on all attributes in CC_j, and returns plaintext.

3.3 Access Control Models

Access Control is an important feature to ensure the security in cloud storage. Access control [11] is generally a procedure that allows or restricts access to a system. It may monitor and record all attempts made to access a system.

Due to differences in requirements of military and commercial security policies, two different kinds of policies had to be developed and this led to the invention of access control models that are Mandatory Access Control (MAC), the Discretionary Access Control (DAC). These models have some flaws which led to the proposal of other models such as Role Based Access Control (RBAC). All these models are known as identity based access control models. In these models, user (subjects) and resources (objects) are identified by unique names. Identification may be done directly or through roles assigned to the subjects. These access control methods are effective in unchangeable distributed system, where there are only aset of Users with a known set of services.

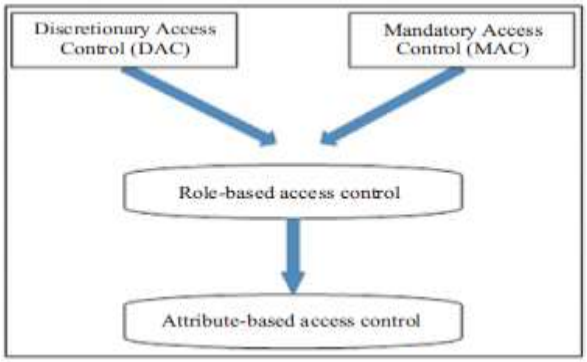

Fig. 3: Access Control Models

Figure above shows the main traditional access control models in cloud computing environment. Each of them have its own significance in different situation and security requirements.

3.3.1 *Discretionary Access Control(DAC) Model*

The Disecrtionary Access Control model, provides the ability to user for restrict their information in the objects, based on user's identity or a membership in a certain group.

DAC is less secure than any other access control model particularly as compared to MAC, so it is used in environments that do not require a high level of security. However DAC is used in commercial operating systems such as UNIX and Windows based platforms. There are two ways to implement a discretionary access control model, this can be achieved via identitybased access control or by means of an access control matrix (Access Control List).

Figure shows the sample model for DAC.

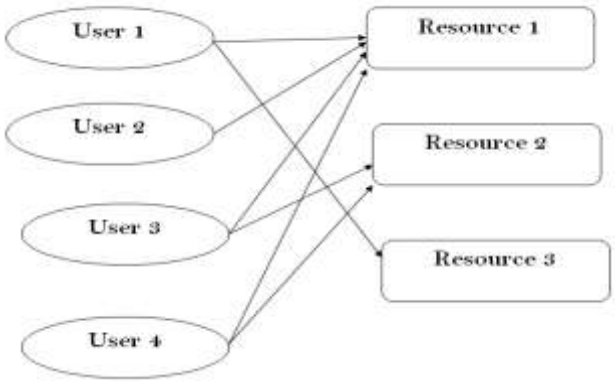

Fig.4: A Sample model for DAC

3.3.2 Mandatory Access Control(MAC)Mode

In mandatory access control model centra permission to a subject that request access to an information in objects. In order to secure access to objects and the information that flows between objects, MAC assigns an access class to each subject and object. An access class is a security level that is used to secure the flow of information between objects and subjects with dominance relationship.

For example, if resource RS comes under extremely sensitive resource in a company, it has been assigned a "Top Secrete" security degree/level. The users, who are in lower level, when attempt to access the resource (RS), he/she will not able to gain access because the mismatch in the security level.

The early formula and most well-known relationships were proposed by Bell and LaPadula (1973) [12]. This model is also known as multilevel security and uses only two properties "no-read-up" and "no-write-down". The BelleLaPadula model has concentrated on securing and controlling data flow.

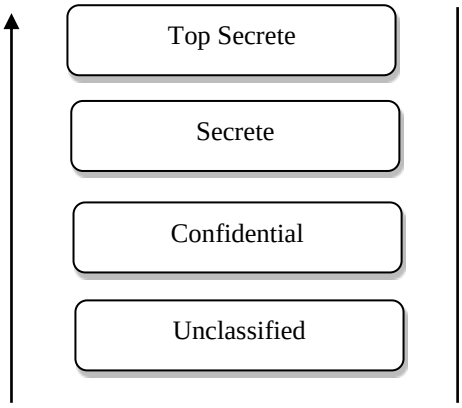

Fig. 5: A Sample Model for MAC

Whereas Top secrete is highest security level and Unclassified indicates lowest security level.

3.3.3 Role Based Access Control(RBAC)

In RBAC [13], access resolution is based on individual or group of user responsibilities and role in the cloud environment. The motivation behind RBAC comes from considering "a subject's responsibility is more important than whom the subject is" [14]. In the RBAC model, a subject can have more than one role or be a member of multiple groups. For example, an employee within an organization can be a member in secretaries group and employees group. Task-Role Based Access Control (T-RBAC) model is another access control approach that has been proposed, which is based upon the RBAC model. However, it assigns permissions to tasks instead of roles. Figure shows the basic model of RBAC.

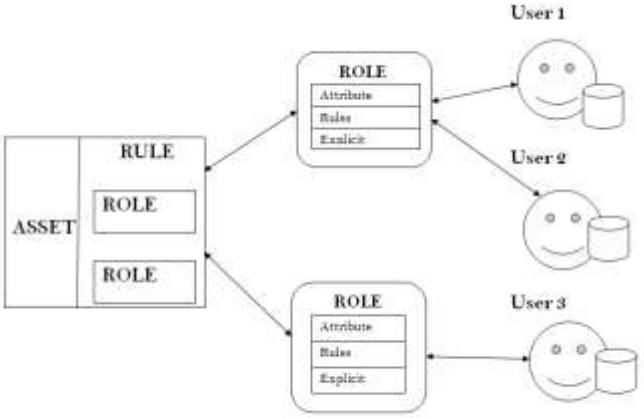

Fig.6: A Sample model for RBAC

3.3.4 Attribute Based Access Control(ABAC)

In ABAC a set of attributes associated with a requester or a resource to be accessed in order to make access decisions. The main difference of other access models with ABAC is the concept of policies that express a complex Boolean rule set, that can evaluate many different attributes. While it is possible to achieve ABAC objectives using RBAC[16]. Another problem with ACL or RBAC models is, if the AC requirement is changed, it may be difficult to identify all the places where the ACL or RBAC implementation needs to be updated. National Institute of Standards and Technology (NIST) [15] released Special Publication (SP) 800-162, "*Guide to Attribute Based Access Control (ABAC) Definition and Considerations"*. describes the functional components of ABAC, as well as a set of issues for employing ABAC within a large enterprise without directly addressing authenticationmechanismsdesign, implementation, and operational considerations for employing ABAC within an enterprise to improve data sharing while maintaining control of that data access.

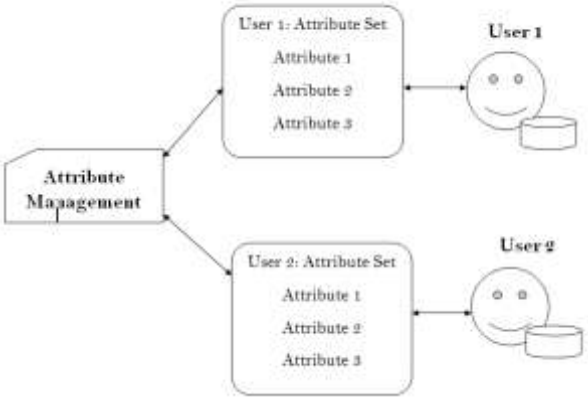

Fig. 7: A Sample Model for ABAC

Here is a comparison of ABE in terms of features supported shown in Table 1. And comparison of traditional Access Control models shown in Table 2.

Table 1: Comparative analysis of ABE schemes

Features	ABE	KP-ABE	CP-ABE	HABE
Fine grained access	Low	Low	Average	Good
Efficiency	Average	Average	Average	Flexible
Computational Overhead	High	High	Average	Average

Table 2: Comparative analysis of Access Control Models

Access Control Parameters	DAC	MAC	RBAC	ABAC
Performance	Less	Depends on security level	Good	Good
Authentication Failure	Less	Based on distributed environment	Based on job role	Less

IV. PROPOSED WORK

To achieve unbreakable security of document we are going to proposed modified attribute based encryption scheme which uses time varying encryption algorithm for document encryption under the environment of Attribute Based Access Control model. Access permissions data is stored separately in metadata file which is an xml file. This file is interlinked with encrypted document. Thus securing the data on untrusted cloud by maintaining flexibility in processing.

V. CONCLUSION

In this paper we have discussed ABE with necessary mathematical background in terms of bilinear map, security assumption on which every ABE system is withstand, broad classification of ABE schemes with their algorithms and drawbacks and then traditional access control models used in cloud for data access with the help of their sample model figures. Also comparative analysis of ABE schemes and access control models are shown in Table 1 and Table 2.

Finally we discussed proposed work, which we will be then evaluated with existing scheme in terms of modification time require to update access permissions in ABAC.

REFERENCES

[1]. "Identity-based cryptosystems and signature schemes," in Advancesin cryptology. Springer, 1985, pp. 47–53.

[2]. Joux, "Introduction to identity-based cryptography," Identity- BasedCryptography, 2009.

[3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE, 2007, pp. 321–334.

[4]. Whitfield Diffie And Martin Hellman, "New Directions in Cryptography", IEEE transactions on information theory, vol. it-22, no. 6, november 1976

[5]. Amit Sahai and Brent Waters, "Fuzzy identity-based encryption," in EUROCRYPT 2005, ser. LNCS, vol. 3494, 2005, pp. 457–473.

[6]. R. Sandhu, E. Coyne, H. Fenstein, and C. Youman, "Role-based access control models," IEEE Computer , vol. 29, no. 2, pp. 38–47, 1996

[7]. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data. Avaialble at: http://eprint.iacr.org/2006/.

[8]. V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute Based Encryption for Fine-Grained Access Conrol of Encrypted Data. Avaialble at: http://eprint.iacr.org/2006/.

[9]. R. Ostrovsky, A. Sahai and B.Waters, "Attribute-based encryption with non-monotonic access structures", in *Proceedings of the 14th ACM conference on Computer and communications security. ACM*, 2014, pp. 195–203.

[10]. Guojun Wnag, Qin Liu and Jie Wu, Hierarchial Attribute-based Encryption for Fine-Grained Access Control in Cloud Storage

[11]. Ausanka-Crues R. Methods for access control: advances and limitations. Harvey Mudd College; 2004. Retrieved December 07, 2012, Available : http://www.cs.hmc.edu/wmike/public_html/courses/security/s06/projects/ryan.pdf.

[12]. Bell D, LaPadula L. Secure computer systems: mathematical foundations. Bedford, MA. Retrieved February 04, 2013, from, http://www.albany.edu/acc/courses/ia/classics/belllapadula1. pdf; 1973.

[13]. Ferraiolo DF, Barkley JF, Kuhn DR. A role-based access control model and reference implementation within a corporate intranet. ACM Trans Inf Syst Secur 1999;2(1):34e64. http:// dx.doi.org/10.1145/300830.300834

[14]. Laurie B. Access control (v0. 1); 2009. Retrieved December 07, 2012, from http://www.links.org/files/capabilities.pdf

[15]. Guide to Attribute Based Access Control, Definitions and Consideration Availabe at: http://dx.doi.org/10.6028/NIST.SP.800-162

[16]. A Younis, K. Kifayat, Madjid Merabti , "A access control model for cloud computing" Available:http://dx.doi.org/10.1016/j.jisa.2014.04.003