IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Secured and Authenticated Anonymous Data Access on Cloud in MANET

Miss. Pooja D.Bardiya[1], Prof. P.L. Ramteke[2]

Student, M.E (CS&IT), H.V.P.M C.O.E.T, Amravati, India[1]

HOD, CS&IT, H.V.P.M C.O.E.T, Amravati, India[2]

Abstract: This Mobile cloud computing (MCC) at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client Mobile Cloud Computing usually consists of front-end users who possess mobile devices and back-end cloud servers During the period between uploading and downloading files (data), the privacy and integrity of files need to be guaranteed. Access control in clouds is gaining attention because it is Important that only authorized users have access to valid Service. Attribute-based access control (ABAC) in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data. This research paper consists of the security of ABE and ABS Algorithm. Using ABE, the records are encrypted under some access policy and stored in the cloud. Users are given sets of attributes and corresponding keys. Only when the users have matching set of attributes, can they decrypt the information stored in the cloud. In ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an authorized one, without revealing its identity. Other users or the cloud can verify the user and the validity of the message stored. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud. There are two type of authentication provided that is from trustee side in terms of token and KDC in terms of skey and pkey.

Keywords: Mobile Cloud Computing, MANET, Attribute based Encryption (ABE), Attribute Based Signature (ABS), Proposed Architecture.

I. INTRODUCTION

Mobile cloud computing is a technique or model in which mobile applications are built, powered and hosted using cloud computing technology. A mobile cloud approach enables developers to build applications designed specifically for mobile users without being bound by the mobile operating system and the computing or memory capacity of the smartphone. Mobile cloud computing centred are generally accessed via a mobile browser from a remote web server, typically without the need for installing a client application on the recipient phone .There are various reasons why mobile cloud computing is evolved as the need for mobile user and especially for the IT users, in the corporate world where mobility is advantages to access the data, users for access the data large scale for their storage and security. Some of them are

- Mobile devices face many resource challenges (battery life, storage, bandwidth etc.)
- Cloud computing offers advantages to users by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on-demand fashion.
- Mobile cloud computing provides mobile users with data storage and processing services in clouds, obviating the need to have a powerful device configuration (e.g. CPU speed, memory capacity etc), as all resource-intensive computing can be performed in the cloud.

Mobile cloud computing is also not fictional. In fact, it's one of today's hottest new technology markets. Gartner predicts that mobile cloud computing will reach a market value of US$9.5 billion by 2014. According to a recent study by ABI Research, more than 240 million businesses will use cloud services through mobile devices by 2015. That traction will push the revenue of mobile cloud computing to $5.2 billion. Mobile cloud computing is a highly promising trend for the future of mobile computing.

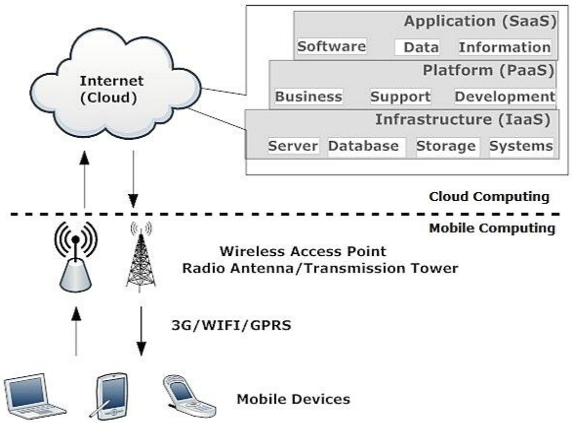


Fig 1: Architecture of mobile cloud computing

- Mobile devices are connected to the mobile networks via base stations that establish and control the connections and functional interfaces between the networks and mobile devices.

DOI 10.17148/IJARCCE.2015.41229

- Mobile users' requests and information are transmitted to the central processors that are connected to servers providing mobile network services.
- The subscribers' requests are delivered to a cloud through the Internet.
- In the cloud, cloud controllers process the requests to provide mobile users with the corresponding cloud services.

Advantages of Mobile Cloud Computing

1. Extending battery lifetime:

- Computation offloading migrates large computations and complex processing from resource-limited devices (i.e., mobile devices) to resourceful machines (i.e., servers in clouds).
- Remote application execution can save energy significantly.
- Many mobile applications take advantages from task migration and remote processing.

2. Improving data storage capacity and processing power:

- MCC enables mobile users to store/access large data on the cloud.
- MCC helps reduce the running cost for computation intensive applications.
- Mobile applications are not constrained by storage capacity on the devices because their data now is stored on the cloud

3. Improving reliability and availability:

- Keeping data and application in the clouds reduces the chance of lost on the mobile devices.
- MCC can be designed as a comprehensive data security model for both service providers and users:

✓ Protect copyrighted digital contents in clouds.
✓ Provide security services such as virus scanning, malicious code detection, authentication for mobile users.

- With data and services in the clouds, then are always (almost) available even when the users are moving.

4. Dynamic provisioning:

- Dynamic on-demand provisioning of resources on a fine-grained, self-service basis
- No need for advanced reservation

5. Scalability:

- Mobile applications can be performed and scaled to meet the unpredictable user demands
- Service providers can easily add and expand a service

6. Multi-tenancy:

- Service providers can share the resources and costs to support a variety of applications and large no. of users.

7. Ease of Integration:

- Multiple services from different providers can be integrated easily through the cloud and the Internet to meet the users' demands.

Thanks to the success of companies like Amazon and SalesForce.com (and of course IBM and the developer Works Cloud zone), many people are familiar with the term cloud computing. However, fewer people understand how mobile cloud computing is different. Mobile cloud computing shares with cloud computing the notion that some level of services is provided by a cloud and accessed by mobile platforms. This paper discusses of mobile cloud computing and cloud computing and the services of SaaS as a services and provide with the architecture studied in detail later.

II. MOTIVATON

MOBILE devices have become an essential part of our daily life. Their portability is well appreciated by end-users and smartphones sales will soon surpass desktop sales. As mobile device popularity grows, end-user demands to run heavier applications are equally increasing. Nowadays, both hardware and software of mobile devices get greater improvement than before, some smartphones such as iPhone 4S, Android serials, Windows Mobile serials and Blackberry, are no longer just traditional mobile phones with conversation, SMS, Email and website browser, but are daily necessities to users.
Cloud computing has now become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Cloud vendors are experiencing growth rates of 50% per annum cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. Cloud services can greatly enhance the computing capability of mobile devices. Mobile users can rely on the cloud to perform computationally intensive operations such as searching, data mining, and multimedia processing.

The use of mobile devices to establish ad-hoc communication systems is a viable solution that provides global connectivity to support a broad range of applications. With the development of wireless access technologies such as 3/4G, LTE, and WiMax, mobile devices can gain access to the network core over longer distances and larger bandwidths. This allows for very effective communication between mobile devices and the cloud infrastructure.

Ad hoc networks are multi-hop network that use wireless communication for transmission without any fixed infrastructure. The networks are form and deform on-the-fly without the need for any system. Ad hoc structure does not require an access point, it is easy to setup, especially in a small or temporary network. Each node in the network forwards the packet without the need of central administration. In ad hoc network, node acts as a router to send and receive the data. An advantage of the system is robustness, flexibility and mobility. Ad hoc network are capable for analyzing radio propagation environment to optimize the performance.

The advantages of an ad hoc network include:

DOI 10.17148/IJARCCE.2015.41229

- Separation from central network administration.
- Self-configuring nodes are also routers.
- Self-healing through continuous re-configuration.
- Scalability incorporates the addition of more nodes.
- Mobility allows ad hoc networks created on the fly in any situation where there are multiple wireless devices.
- Flexible ad hoc can be temporarily setup at anytime, in any place.
- Lower getting-started costs due to decentralized administration.
- The nodes in ad hoc network need not rely on any hardware and software. So, it can be connected and communicated quickly.

The objective of our research is to use a systematic approach to investigate both cloud computing and mobile ad hoc networks (MANETs) technologies in order to understand the capability of cloud computing for securing MANET applications. This research work consisting of mobile computing and cloud computing, which provide cloud based services to users through the Internet and mobile devices.

III. OBJECTIVES PROPOSED

The main Objective of this paper is the following:

[1]Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
[2]The identity of the user is protected from the cloud during authentication.
[3]The architecture is decentralized, meaning that there can be several KDCs for key management.
[4]The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.
[5]Revoked users cannot access data after they have been revoked.
[6]The protocol supports multiple read and writes on the data stored in the cloud.
[7]The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.
[8] Mobile is used as the way of accessing file on data in the presence of the Ad-Hoc Network between cloud and multiple mobile users

IV. MOBILE AD-HOC NETWORKS (MANETS)

The increasing use wireless portable devices such as phones and laptops is leading to the possibility for spontaneous or ad hoc wireless communication known as Mobile Ad Hoc Networks (MANET). A mobile Ad hoc network (MANET) is a self-configuring network that does not require any pre-existent (fixed) Infrastructure, which minimizes their deployment time as well as cost. As each node in this network is free to move which makes the network to change its topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network on the fly as shown in Fig. Mobile Ad-Hoc Network (MANET) is one of the most active research topics during the last ten years. With the advances in wireless technologies and development of mobile devices, ad hoc networks will play an important role in enabling present and future communication. For both video and data communication, mobile radio technologies has experienced a rapid growth. A MANET is a dynamic wireless network formed by a set of mobile hosts which communicate among themselves by means of the air without any pre-existing infrastructure. Each node in the MANET can act as a router as well as host. In order to maintain connectivity in a mobile ad-hoc network all participating nodes have to perform routing of network traffic. The success of communication highly depends on other nodes cooperation. Therefore, MANET has the property of rapid infrastructure-less deployment and no centralized controller which makes it convenient to people and vehicles can thus be internet-worked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension. By extending range of mobile nodes ad hoc networks supports multi-hop routing by which they can extend the range of wireless networks. Range depends upon the concentration of wireless users.

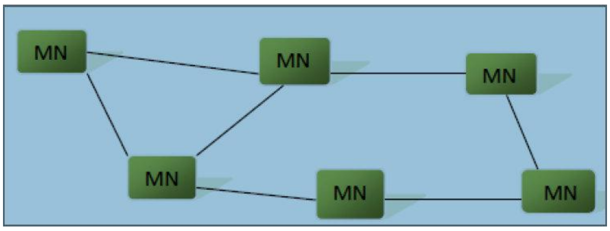


Fig 2: Mobile Ad-Hoc Networks

A. Characteristics of MANET

Mobile ad hoc network is a collection of autonomous and mobile elements such as laptop, smart phone, tablet PC etc. The mobile nodes can dynamically self-organize in arbitrary temporary network topology. There is no preset infrastructure thus it does not have the clear boundary. Some main characteristics of MANET are discussed below:

Infrastructure less: MANET is an infrastructure less system which has no central server, or specialized hardware and fixed routers. All communications between nodes are provided only by wireless connectivity.

Wireless Links: Wireless links make Mobile Ad Hoc Network unreliable and susceptible to various kinds of attacks. Because of limited power supply of wireless nodes and mobility of nodes, the wireless links between those nodes in the mobile ad hoc network are not consistent for communication participants.

Node Movement: Mobile nodes are autonomous units in network which continuously change their position and topology independently. Due to continuous motion of nodes the topology changes frequently which mean tracking down of particular node become difficult. The nodes can easily come out of or into the radio range of

DOI 10.17148/IJARCCE.2015.41229

various other nodes. The routing information of nodes changes continuously as their movement becomes random.

Power limitation: The mobile hosts are small and light weight. They are supplied by limited power resources such as small batteries. This limitation causes vulnerability namely when attackers may target some node batteries to disconnect them, that may lead to network partition. Some attacks may try to engage the mobile nodes un-necessarily, so that they keep on using their battery for early drainage.

Dynamic topologies: Nodes are free to move arbitrarily, thus the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.

Self-Configuring: MANET has decentralized infrastructure, with all mobile nodes functioning as routers and all wireless devices being interconnected to one another. MANET is a self-configuring network in which network activities, including the discovery of the topology and delivery of messages, are executed by the nodes themselves.

B. Advantages of MANET

Router Free: Connecting to the internet without the need for a wireless router is the main advantage of using an ad hoc network. Because of this, running an ad hoc network can be more affordable than traditional network because we don’t have the added cost of a router.

Mobility: The wireless mobile nodes can move at the same time in different directions. Although the routing algorithm can deal with this issue, the performance simulations show that there is a threshold level of node mobility such that protocol operation begins to fail.

Speed: Creating an ad hoc network from scratch requires a few settings changes and no additional hardware or software. If you need to connect multiple computers quickly and easily, then an ad hoc network is an ideal solution.

Fault Tolerance: MANET supports connection failures, because routing and transmission protocols are designed to manage these situations.

Connectivity: The use of centralized points or gateways is not necessary for the communication within the MANET, due to the collaboration between nodes in the task of delivering packets.

Fast Installation: The level of flexibility for setting up MANET is high, since they do not require any previous installation or infrastructure and, thus, they cab be brought up and torn down in a very short time.

Cost: MANET could be more economical in some cases as they eliminate fixed infrastructure costs and reduce power consumptions at mobile nodes.

V. ARCHITECTURE OF PROPOSED SYSTEM

Mobile cloud computing is the technique of merging two technology together and overcome some of the disadvantages of each other and get the benefits of each other together. as cloud computing is evolved as the emerging technology and has become popular due to the services offered neglecting the drawbacks of the risk to data security before putting a job into the cloud and the risks of data and programs are safe in provider’s premises and many more. As it is said that that every coin has two sides ‘head’ and ‘tail’. If drawback is one side than its features services, different models as per requirement and low cost and save money approaches has made it the stand alone technology.

Mobile has increased its population due to its increasing features day-by-day and advancement in the techniques and overcoming some of the drawbacks as the previous versions recently 4g has become the part of the telecommunication technology that has lead to the fast mode of communication with the advanced features.

When the researchers tried to connect the two technologies of cloud and mobile computing together and made the invention of mobile cloud technology .this was possible due to the presence of the most important method of connecting in any part of the world is internet .internet is the gateway success that has created the ways to connect and create successes. In mobile cloud computing internet has become the glue the binds together. But yes it is the pay on use way of communication.

Here in this paper we have use the MANET as the medium of communication. MANET is the costless, infrastructure less, Wireless Links, support mobility in the range technique of communication but has the advantages in the limited range of mobile wireless communication depends on the range of the router.

The proposed architecture is the combination of cloud and Mobile in MANET .It provides the way to access the saas of cloud in limited range example in the range of college hospitals organization offices etc. for example let us consider the college campus there are different departments, staffs, administrator department, training and placement department and of course student section, library section etc. Now admin department wants to held a meeting about the upcoming events in the different section of college .there will be either the notice be displayed on the notice board or follow the tree structure to send the information as admin->HOD->Professors->staff .here there will be the waste of time in writing notice ,printing ,sending in different department and storage of paper for each and every meeting for at least week. Instead of doing so we can use cloud for the storage and mobile MANET can be used as the medium of sending data to different section and to the last person to be called in just on e upload button of file. There can be the possibility that there is change in the notice but it then become impossible to send to different section or there might be the situation that there is the notice to be send just in 15 min to attend the meeting in such case the architecture is useful.

Security and Authentication is the important part when send receiving and storage of data is concerned. Here we have provided the two methods of security and double authentication. Security of file is provided by the ABE and ABS algorithm and authentication is provided by the two trusted party called trustee and KDC. The ABE and ABS algorithm are studied in the later section of this paper. It

DOI 10.17148/IJARCCE.2015.41229

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

has one of the important part that concerns to the access rights of the user as creator, reader and writer. Depending on the access rights user can perform his/her functions .creator can only upload ,download and read his own file ,writer has the rights of modify the uploaded file by the creator after full authentication, read and download the file and reader can on read and download the file.

Fig shows the architecture that consists of the following steps:
Step1: users will signup according to the access rights
Step 2: user needs the token to authenticate himself from the trustee and request for the token to the trustee
Step3: trustee sends the token to the user after verifying the set of attributes he has given at the time of signup, till then user is in the waiting state.
Step 4: then the user asks for the secret key and the private key to the KDC .This skey and pkey is used for the encryption and decryption of file.
Step 5: Until the KDC sends it the user cannot encrypt the file and decrypt the file.
Step 6: This is the last phase of the user where the user can access the file as per the rights granted to the user at the time of sign up

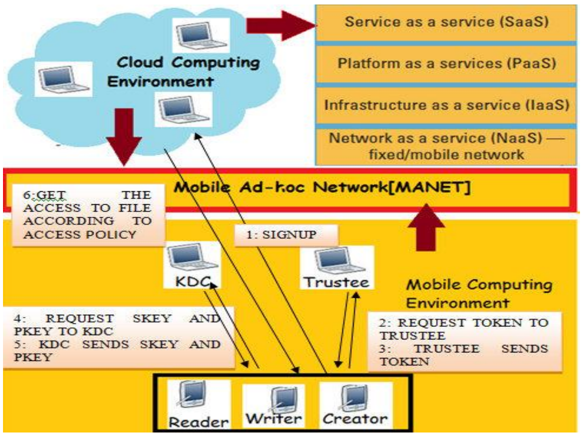

Cloud Computing Environment
Service as a service (SaaS)
Platform as a services (PaaS)
Infrastructure as a service (IaaS)
Network as a service (NaaS) — fixed/mobile network
Mobile Ad-hoc Network[MANET]
6:GET THE ACCESS TO FILE ACCORDING TO ACCESS POLICY
1: SIGNUP
KDC
Trustee
Mobile Computing Environment
4: REQUEST SKEY AND PKEY TO KDC
5: KDC SENDS SKEY AND PKEY
2: REQUEST TOKEN TO TRUSTEE
3: TRUSTEE SENDS TOKEN
Reader
Writer
Creator

Fig 3: Architecture of the Proposed System

A. Advantages of the System

1. This Application Software consists of double Authentication Process through the trustee and respective KDC
2. User has to signup according to the access rights i.e user can be the creator /reader/writer and the access to the data is restricted.
3. It has the main advantages of multiple read at the same time, multiple modifications to the uploaded data and can upload multiple file according to the rights granted to the user.
4. It helps to reduce the paper work involved in many situations like notices, test paper, meetings notification, etc.
5. It helps to reduce time and storage as the cloud is used 'Anytime and Anywhere'.
6. ABE is used as the means of securing the data files of owner according to the access policy.
7. Again, the encryption and decryption of file is provided by the skey and pkey generated by the Respective KDC which is not needed to be remembered automatically generated.
8. Admin is provided which has the power of analysis of users created; file uploaded by respective creator and has the right to delete the user if that user is not required.
9. The revoked user user is not able to access the file once he is deleted.

VI. PROPOSED ALGORITHM

ABE Attributed based encryption (ABE), first introduced by Sahai and Waters, and provides a mechanism by which we can ensure that even if the storage is compromised, the loss of information will only be minimal. What attribute based encryption does is that, it effectively binds the access-control policy to the data and the users (clients) instead of having a server mediating access to files. To understand this better, we will take a closer look into what access control is. Access Policy. An access control policy would be a policy that denotes the kind of users who would have permissions to read the documents. e.g In an academic setting, grade-sheets of a class may be accessible only to a professor handling the course and some teaching assistants (TAs) of that course. We can express such a policy in terms of a predicate:

$$\text{((Professor} \wedge \text{CS dept.)} \\ \text{or} \\ \text{(M.tech student} \wedge \text{course TA} \wedge \text{CS dept.))}$$

We will call the various credentials (or variables) of the predicate as attributes and the predicate itself which represents the access policy as the access-structure. In the example here the access structure is quite simple. But in reality, access policies may be quite complex and may involve a large number of attributes. Properties. There are two major features to attribute based encryption:

1. It has the capacity to address complex access control policies.
2. The exact list of users need not be known apriori. Knowledge of the access policy is sufficient.

Also, an important property that attributes based encryption schemes must satisfy is that of collusion resistance. Collusion resistance means that, if 2 or more users possessing different keys combine to decrypt the ciphertext, they will be successful if and only if any one of the users could have decrypted it individually. In other words, even if multiple parties collude, they should not be able to decrypt the ciphertext unless one of them was able to decrypt it completely by herself. These properties ensure that only users possessing the right keys have access to the information. Moreover, as the encryption is based on the access-structure it implicitly assures anonymous access control.

A. Attribute-Based Encryption

[1] System Initialization
Select a prime q, generator g of G0 , groups G0 and GT of order q, a map $e : G0 \times G0 \rightarrow GT$, and a hash function $H : \{0; 1\}^* \longrightarrow G_0$ that maps the identities of users to G0 . The hash function used here is

DOI 10.17148/IJARCCE.2015.41229

SHA-1. Each KDC Aj ϵ A has a set of attributes Lj. The attributes disjoint (Li∩Lj=Φ for (i ≠ j). Each KDC also chooses two random exponents αi , yi ϵ ZZq . The secret key of KDC Aj is

SK[j] = {αi, yi, iϵ Lj} (1)

The public key of KDC Aj is published

PK[j] = {e (g, g)αi ,gyi ,i ϵ Lj } (2)

[2] Key Generation and Distribution by KDCs
User Uu receives a set of attributes I [j, u] from KDC Aj , and corresponding secret key s k i ,u for each i 2 I[j, u]

s k i ,u =g α i H(u)yi ; (3)

Where αi , yi ϵ sk[j] . Note that all keys are delivered to the user securely using the user's public key, such that only that user can decrypt it using its secret key.

[3] Encryption by Sender
The encryption function is ABE. Encrypt (MSG, X). Sender decides about the access tree X. LSSS matrix R can be derived as in[10]. Sender encrypts message MSG as follows:

1. Choose a random seed s 2 ZZq and a random vector v ϵ ZZh , with s as its first entry; h is the number of leaves in the access tree (equal to the number of rows in the corresponding matrix R).
2. Calculate λx= Rx v, where Rx is a row of R choose a random vector wϵ ZZh with 0 as the first entry.
4. Calculate wx=Rx w.
5. For each row Rx of R, choose a random $\rho_x \in \mathbb{Z}_q$.
6. The following parameters are calculated:

$$\begin{aligned}&c0=MSG\ e(g,g)^{\alpha}\\&c_{1,x}=e(g, g)^{\lambda x}\ e(g, g)\alpha(x)^{\rho x},\forall x\\&c_{2,x}=g^{\rho x}\forall x \qquad (4)\\&c_{3,x}=g^{yxs}(x)^{\rho x}\ g^{wx},\forall x\end{aligned}$$

Where Π(x) is mapping from Rx to the attribute i that is located at the corresponding leaf of the access tree.
7. The cipher text C is sent by the sender (it also Includes the access tree via R matrix):

C=(R,Π, C0,{C1,x,C2,x,C3,x,∀x}) (5)

[4] Decryption by Receiver
The decryption function is ABE: Decrypt(C, {s k i, u}), where C is given by (5). Receiver Uu takes as input ciphertext C, secret keys {s k i, u}, group G0 , and outputs message msg. It obtains the access matrix R and mapping from C. It then executes the following steps:

1. U u calculates the set of attributes {π (x): x ∈ X}∩ Iu That is common to itself and the access matrix. X is the set of rows of R.
2. For each of these attributes, it checks if there is a subset X' of rows of R, such that the vector (1, 0. . . 0) is their linear combination. If not, Decryption is impossible. If yes, it calculates constants cx ϵZ q, such that

Σ x ϵ x' cx Rx = (1,0,….,0).

3. Decryption proceeds as follows:
a. For each xϵX', dec(x) $=\frac{c(1,x)\ e(H(u),c(3,x))}{e(sk(x)u,c(2,x))}$
b. U u Computes MSG=C0/πxϵx' dec(x)

The concept of ABE (attribute based encryption) was first introduced by Amit Sahai et al., [19], later they have come out with several ABE based works [20, 21, 22, and 23].In [20] a new method for constructing ABE system for circuits using multi linear maps had been proposed and proved to be better than both CP-ABE and KP-ABE.

A. Attribute-Based Signature Scheme

[1] System Initialization
Select a prime q, and groups G1 and G2, which are of order q. We define the mapping e^: G1 × G1 → G2. Let g1 , g2 be generators of G1 and hj be generators of G2 , for j ϵ[tmax], for arbitrary tmax . Let H be a hash function. Let A0 = ha0 ,where a0 ϵ Zq*is chosen at random.(TSig, TVer) mean TSig is the private key with which a message is signed and TVer is the public key used for certification .the secret key for the trustee is TSK=(a0,TSig) and public key is TPK =(G1,G2, H,g1,A0, h0,h1,.., htmax,g2,TVer).

[2] User Registration
For a user with identity U u the KDC draws at random

K base ϵ G.

Let K0 = Kbase1/a0
q
The following token γ is output

γ= (u, Kbase, K0, ρ), (6)

Where ρ is signature on u‖ Kbase using the signing key TSig.

[3] KDC setup
Choose a, b ϵ Z_q^* randomly and compute:

A ij=h_{ij}^{a} , B ij=h_j^{b}, for Ai ϵ A, jϵ [t max].

The private key of ith KDC is

ASK[i] = (a, b)

And public key

APK[i] (A ij, B i j | ϵ[t max]).

[4] Attribute generation
The token verification algorithm verifies the signature contained in γusing the signature verification key TVer in TPK. This algorithm extracts K base from γ using (a,b)from ASK[i] and computes Kx=$K_{base}^{\frac{1}{(a+bx)}}$,xϵJ[i, u].the key K x can be checked for consistency using algorithm ABS.KeyCheck(TPK,APK[i],γ,K x) which checks

ê (K x, A ij B_{ij}^{x})= ê(K base, h j),

For all xϵJ [i, u] and jϵ[tmax]

[5] Sign
The algorithm

ABS.Sign (TPK, {AP K[i] : i ϵ AT[u]},
γ, {Kx: x ϵ Ju}, M SG, Y);

Has input the public key of the trustee, the secret key of the signer, the message to be signed and the policy claim y. The policy claim is first converted into the span program
M ϵ$Z_q^{l\times t}$, with rows labeled with attributes x of M. Let π' denotes the mapping from rows to the attributes .so, π'(x)

DOI 10.17148/IJARCCE.2015.41229

is the mapping from M x to attribute x. A Vector v is computed that satisfies the assignment {x: x ϵ J [i , u]}.compute

$$\mu = H(MSG||y).$$

Choose r0ϵZq* and ri ϵ Z q, J u and compute:

$$Y=K_{base}^{ro} \text{ , } S\ j= (K_i^{u})r0, Si= (K_i^{vi})r0. (g2g_1^{u})ri(\forall j\epsilon\ J\ u), \quad (7)$$

$$W=K_0^{ro} \text{,} Pj=\Pi\ i\ \epsilon\ AT[u]\ (A\ ijB_{ij}^{\Pi'(i)})\ Mij\ ri\ (\forall j\epsilon[t]). \quad (8)$$

The signature is calculated as

$$\sigma = (Y, W, S1, S2, \dots, St, P1, P2, \dots Pt) \quad (9)$$

[F] Verify
The algorithm

ABS. verify(TPK,σ=(Y,W,S1,S2,…,St,P1,P2,…,Pt),MSG, y).
Converts y to the corresponding monotone program $M\epsilon Z_q^{l\times t}$, with rows labeled with attributes .Computes μ = H(MSG||y).if Y=1, ABS. verify=0 meaning false .Otherwise, the following constraints are checked

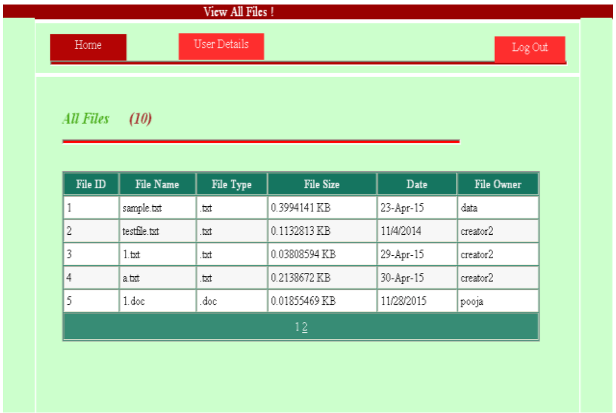
$$\hat{e}\ (W,\ A0) = \hat{e}(Y,h0), \quad (10)$$

$$\Pi\ i\ \epsilon\ l\ \hat{e}\ (S\ i,\ A\ i,j\ B_{i'j}^{\pi'(i)})\ M\ ij\ )= \hat{e}(Y,h1)\ \hat{e}(g2g_1^{\mu},P1),j=1,$$
$$=\hat{e}\ (g2, g_1^{\mu},Pj),j>1, \quad (11)$$

where I'=AT[i].

VII. SYSTEM EXECUTION DETAIL

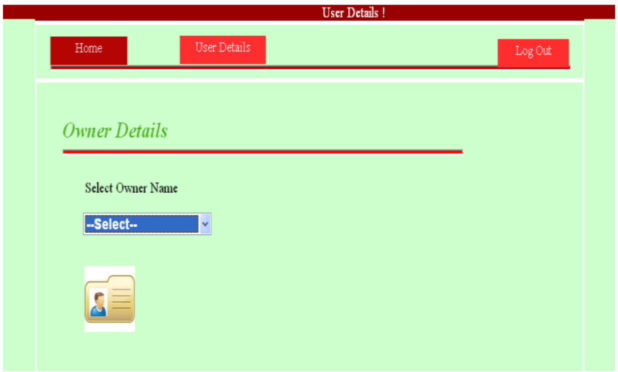
Step1: after login of Admin



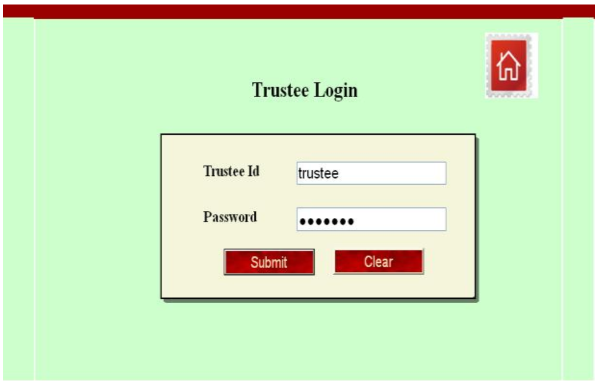
All Files (10)

File ID	File Name	File Type	File Size	Date	File Owner
1	sample.txt	.txt	0.3994141 KB	23-Apr-15	data
2	testfile.txt	.txt	0.1132813 KB	11/4/2014	creator2
3	1.txt	.txt	0.03808594 KB	29-Apr-15	creator2
4	a.txt	.txt	0.2138672 KB	30-Apr-15	creator2
5	1.doc	.doc	0.01855469 KB	11/28/2015	pooja

Admin can Analyse the user the present and accordingly Admin has full right to delete the user

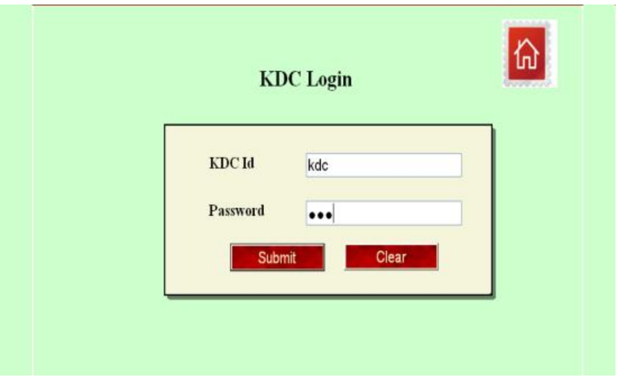


Step 2: Login for Trustee



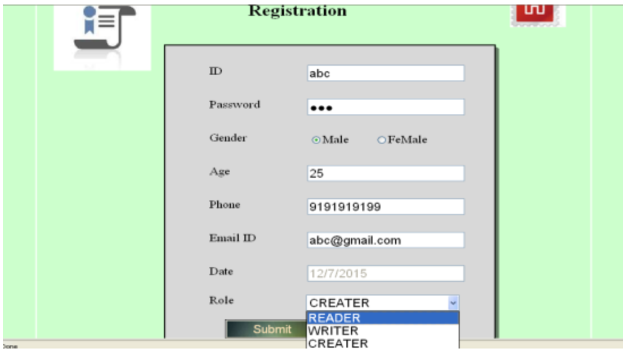
Trustee Id: trustee
Password: •••••••

Step 3: login for KDC



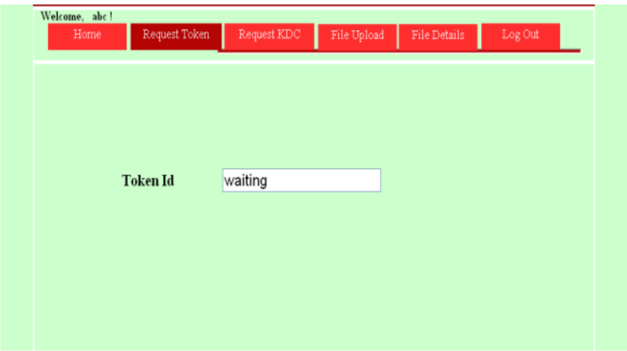
KDC Id: kdc
Password: •••

Step 4: Signup of User creator/writer/reader



ID: abc
Password: •••
Gender: ● Male ○ FeMale
Age: 25
Phone: 9191919199
Email ID: abc@gmail.com
Date: 12/7/2015
Role: CREATER

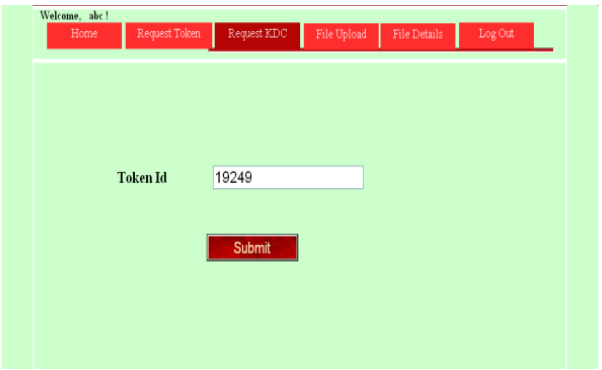
Step 5: User abc Request token to trustee and user before granting token from trustee



Token Id: waiting

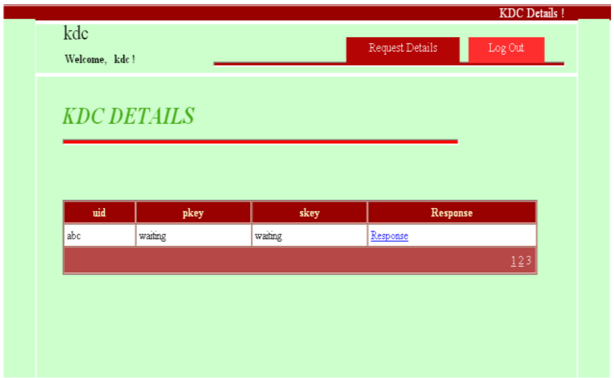
Step 6: user abc request keys for encrypting and decrypting file to KDC by giving the token granted by trustee

DOI 10.17148/IJARCCE.2015.41229



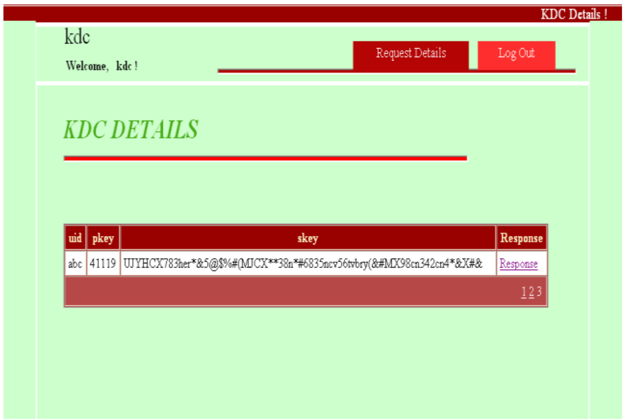
Token Id: 19249

Step 7: User before granting keys from KDC is in waiting state and cannot encrypt and decrypt the file



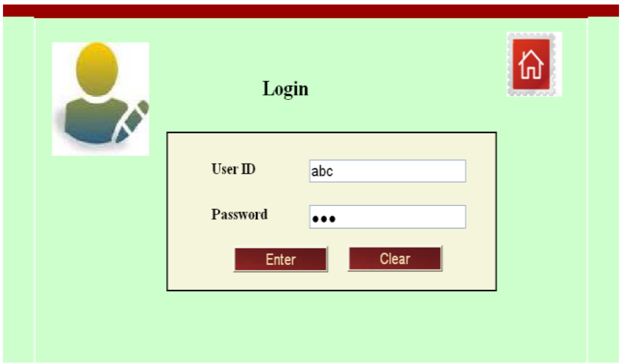
uid	pkey	skey	Response
abc	waiting	waiting	Response
			1 2 3

After granting the keys



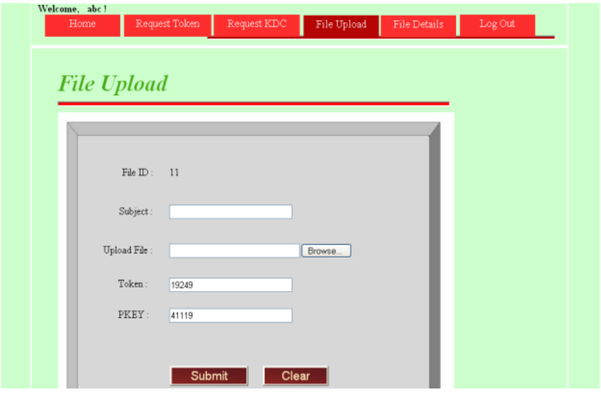
uid	pkey	skey	Response
abc	41119	UJYHCX783her*&5@$%#(MJCX**38n*#6835ncv56tvbry(&#MX98cn342cn4*&X#&	Response
			1 2 3

Step 8: Then once user has authenticated then he/she can access file according to the user's rights



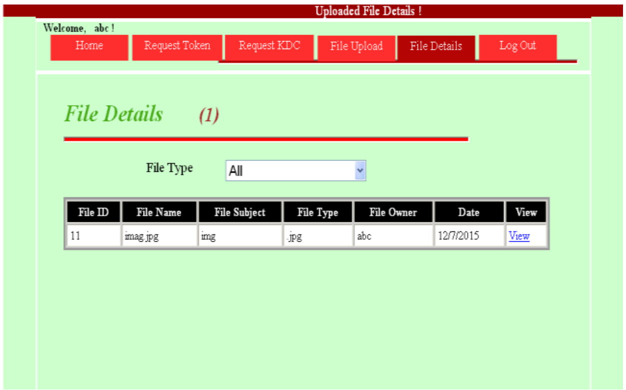
User ID: abc
Password: •••

Step A: user as creator upload file



File ID : 11
Subject :
Upload File :
Token : 19249
PKEY : 41119

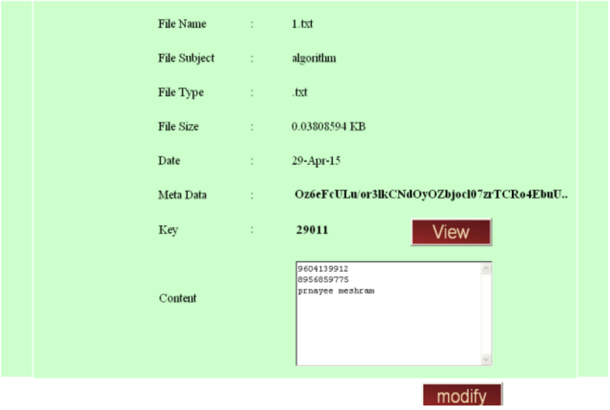
Step B: user as creator view file



File Type: All

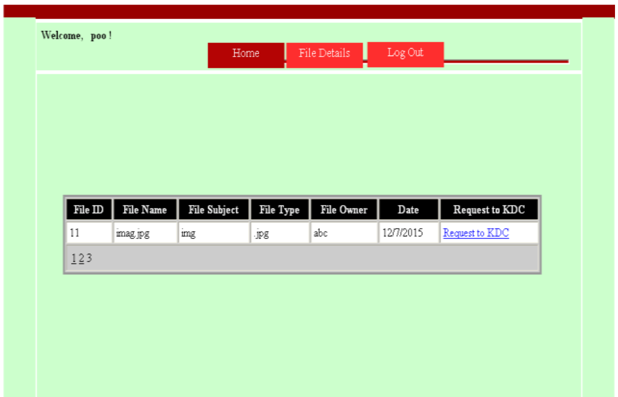
File ID	File Name	File Subject	File Type	File Owner	Date	View
11	imag.jpg	img	.jpg	abc	12/7/2015	View

Step C: Users as Writer modify and file



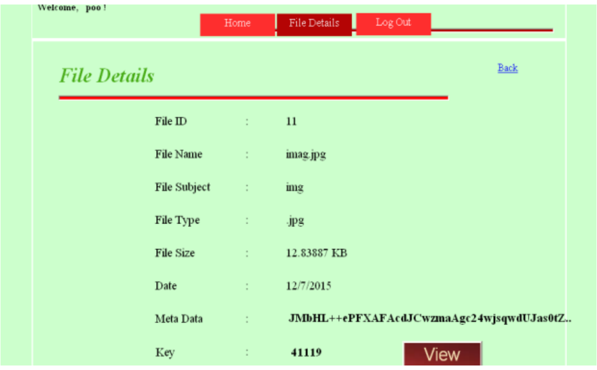
File Name : 1.txt
File Subject : algorithm
File Type : .txt
File Size : 0.03808594 KB
Date : 29-Apr-15
Meta Data : Oz6eFcULu/or3lkCNdOyOZbjocl07zrTCRo4EbuU..
Key : 29011
Content
9604139912
8956859775
prnayee meshram

Step D: User as reader can view



File ID	File Name	File Subject	File Type	File Owner	Date	Request to KDC
11	imag.jpg	img	.jpg	abc	12/7/2015	Request to KDC
1 2 3						

And download the file



Welcome, poo !

File Details

File ID	:	11
File Name	:	imag.jpg
File Subject	:	img
File Type	:	.jpg
File Size	:	12.83887 KB
Date	:	12/7/2015
Meta Data	:	JMbHL++ePFXAFAcdJCwzmaAgc24wjsqwdUJas0tZ..
Key	:	41119

A. Advantages of the Proposed System

1. This Application Software consists of double Authentication Process through the trustee and respective KDC
2. User has to signup according to the access rights i.e user can be the creator /reader/writer and the access to the data is restricted.
3. It has the main advantages of multiple read at the same time, multiple modifications to the uploaded data and can upload multiple file according to the rights granted to the user.
4. It helps to reduce the paper work involved in many situations like test paper, meetings notification, etc.
5. It helps to reduce time and storage as the cloud is used 'Anytime and anywhere'.
6. ABE is used as the means of securing the data files of owner according to the access policy.
7. Again, the encryption and decryption of file is provided by the skey and pkey generated by the Respective KDC which Is not needed to be remembered automatically generated.
8. Admin is provided which has the power of analysis of users created; file uploaded by respective creator and has the right to delete the user if that user is not required.
9. The revoked user user is not able to access the file once he is deleted.

VIII. CONCLUSION

Attribute based encryption is an extensively used technique for access control. It has been used to refine users from accessing information .The primary advantage of ABE is key strength, enabling users to have a stronger encryption, than other encryption. The emerging capabilities of mobile devices and cloud computing have given a new direction to the MANET in the organization level or limits of the router level, which decreases the cost and allow us to use infrastructure wireless networks and infrastructure less wireless networks (i.e. Mobile Ad hoc Wireless Network). Advantages of mobile and cloud can be binded together with the help of MANET and work freely in the MANET environment and overcome many manual work and storage.

REFERENCES

[1] K. Kumar and Y.-H. Lu, "Cloud Computing for Mobile Users: Can Offloading Computation Save Energy?"Computer, vol. 43, no. 4, Apr. 2010, pp. 51–56.

[2] H. T. Dinh et al., "A Survey of Mobile Cloud Computing: Architecture, Applications, and Approaches," Wireless Commun. and Mobile Computing, Oct 2011.

[3] Kavita Taneja, R.B. Patel "An Overview of Mobile Ad hoc Networks: Challenges and Future."

[4] Vikaram Patalbasi, Sonali Mote "Mobile Ad hoc Networks: Opportunities and Future."

[5] Channel Modeling for Vehicle-to-Vehicle Communications and Networking

[6] David W. Matolak (2012). Wireless Technologies in Vehicular Ad Hoc Networks: Present and Future Challenges (pp. 20-47).

[7] D.P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Brooks/Cole Publishing, Aug. 2003.

[8] B. Liu and D. Towsley, "Coverage of Sensor Networks: Fundamental Limits," Proc. Third IEEE Int'l Conf. Mobile Ad Hoc and Sensor Systems (MASS), Oct. 2004.

[9] DjamelDjenouri and LyesKhelladi, "A survey of security issues in mobile ad hoc and sensor network", IEEE communications Surveys and Tutorials journal,Volume 7, Number 4, 2005, pp 2-29.

[10] SushmitaRuj, Milos Stojmenovic and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE, 2014.

[11] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, Apr.- June 2012.

[12] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing, 2009.

[13] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., 2009.

[14] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), 2010.

[15] International Journal of Application or Innovation in Engineering & Management (IJAIEM)

[16] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), 2010.

[17] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), 2010.

[18] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), 2011.

[19] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[20] S.SeenuIropia, R.Vijayalakshmi, "Decentralized Access Control Of Data Stored In Clouds Using Key Policy Attribute Based Encryption", International Journal Of Invention In Computer Science And Engineering, 2014.

[21] R.L. Rivest, A. Shamir, and Y. Tauman, "How to Leak a Secret," Proc. Seventh Int'l Conf. Theory and Application of Cryptology and Information Security (ASIACRYPT), 2001.

[22] X. Boyen, "Mesh Signatures," Proc. 26th Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), 2007.

[23] D. Chaum and E.V. Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), 1991.

[24] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[25] K. Yang, X. Jia, and K. Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IACR Cryptology ePrint Archive, 2012.

[26] W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Cloud Computing Security Workshop (CCSW), 2009.

[27] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," Proc. IEEE 10th Int'l

[28] Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.

[29] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA,S. M. Metev and V.

DOI 10.17148/IJARCCE.2015.41229

P. Veiko, Laser Assisted Micro technology, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[30] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

[31] J.Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute based encryption," in Proc.IEEE Symp. Security and Privacy, Oakland, CA,2007.

[32] A. Sahai and B.Waters,"Fuzzy Identity Based Encryption," In Proc. Advances in Cryptology- Eurocrypt, 2005, vol.3494, pp.457-473.

[33] S. Muller, S. Katzenbeisser, and C. Eckert," Distributed attribute-based encryption," in Proc.11th Int Conf. Information Security and Cryptology, 2008, pp.20- 36, Springer

BIOGRAPHIES

Miss. Pooja D. Bardiya Received the B.E degree in Information Technology and pursuing Masters in computer science and Information Technology from H.V.P.M College of engineering Amravati. Her research study Interest is in Data security and Information security. She has published papers that relates to the data security in cloud computing and she is doing research study secured and authenticated data access in cloud.

Prof. P.L. Ramteke is pursuing Ph.D in Mobile Computing .He is Associate Professor and head of computer science and Information Technology in H.V.P.M College of Engineering Amravati. He has the Specialization in Mobile Computing, Software Engineering, Expert System and Design. He has research experience of 3 years and published & papers in specialized topics above. He is member of various technical Institutes like ISTE, IAPT, and IAI.

DOI 10.17148/IJARCCE.2015.41229