International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 13 (2015)

A framework for Identity and Access Management In HealthCare Cloud

Ms. S.N.Dhanabagyam[1], Dr.G.R.Karpagam[2]

[1]*Phd Scholar (Part Time), Department of Applied Mathematics & Computational Science*
PSG College of Technology, Coimbatore-641 004, India
dhana_bagyam2@yahoo.com
[2]*Professor, Department of Computer Science and Engineering,*
PSG College of Technology, Coimbatore-641 004,
India grkarpagam@gmail.com

Abstract

Identity & Access Management forms a baseline forsharing of essential data in ehealth. Identity management guarantees aneffective authentication; Access management ensures authorization techniques for accessing data or resources or services.This paper proposes a framework for identity management and access control of data in ehealth cloud called **SEIMMAC**(**S**ecured**E**health**I**dentity **M**anagement **M**eta **A**ccess **C**ontrol). SEIMMAC comprises of 7 basicelementsorganized in 3 layers. The seven elements are Patients, Electronic Health Record (EHR), Identitymanagement, MetaAccess Control, Users, Cloning Agent and Cloud.**User layer/**

Application layerfocus on user query andprocessing of user query language.**Security layer** which focus on protocols and methods for ensuring identity and access management such as SSO, SAML, KERBEROS. **Infrastructure layer** concentrates on storage of Electronichealth Record in Ehealth cloud. The proposed framework ascertains availability to the Electronic health record stored in cloud using Attribute Based Encryption and gives fine grained meta access control to the records.

The organization of the paper is as follows Section I gives an introductory concepts ofehealth, SectionII shows therelated works.Section III presents a detail description of proposed frame work of the ehealthsystem. In Section IV security modeland analysis isdiscussed. Section V explains about the prototype implementation. Last section VIconcludes and draws a limeline to future directions.

Keyword: IdentityManagement, Authentication, Accesscontrol, Attribute Based Encryption.

1. Introduction

Due to the wide use of cloud computing in recent days patients data can be monitored or accessed in an emergency by a son or daughter who are living in different geographical zone on their work.They can access the services of ehealth cloud by using the personal attributes as credentials. In ehealth different hospitals(A, B, C) and organizations(X, Y, Z) are registered as service providers;nurses, health workers like group D's, ehealthprofessionals like physicians, lab analysts, radiologists, pathologists, specialized doctors are included as the service providers (Sdp), patients and publics who are in need to access ehealth are the service consumers.Ehealth uses cloud computing via internet is also can be called Ubiquitous health care system.When a patient wants to get service from specialized doctor in hospital B referred from a physician in hospital A would have stored all the medical records of the patient in Ehealth cloud in an encrypted form and to access the particular medical records of the patient, doctor uses the patient information's (patients name, sex, age, etc) as credentials.In this paper to ensure the security features as Confidentiality, Data Integrity and Availability (CIA traid) is proposed.The contributory work is as follows as first is to propose to build a secured framework for the ehealth system.Second to display how an identity management guarantees to provide the authentication and authorization.Next to achieve fine grained access control of patients medical data using attribute based encryption.

Benefits in adoption of cloud computing inehealth

E-Health can benefit from cloud computing and those are cost reduction, scalability, reliability, efficiency and data storage. Resource sharing of different hospital and organization will reduce the cost, time etc. So hospitals can concentrate on their proper health service and leave the job of IT to the trusted vendor with one IT officer to monitor it which saves lot of money spends in IT infrastructure. From the scalability, hospitals can scale up and down their servers and hardware whenever they need and it will reduce the cost of the unused servers and hardware.

Identity and Access Management (IAM)

IAM improves operational efficiency, regulatory compliance management by managing AAA services. Few experts suggested IAM as a Service (IDaaS) [1] to be a new service model to achieve greater security and privacy goals in cloud computing.[2] listed an idea for building IAM as one of the security domain to meet the objectives like privacy, trust, interoperability, CIA traid and self-managed security services. Figure 1 shows the components of IAM involved in Ehealth system.

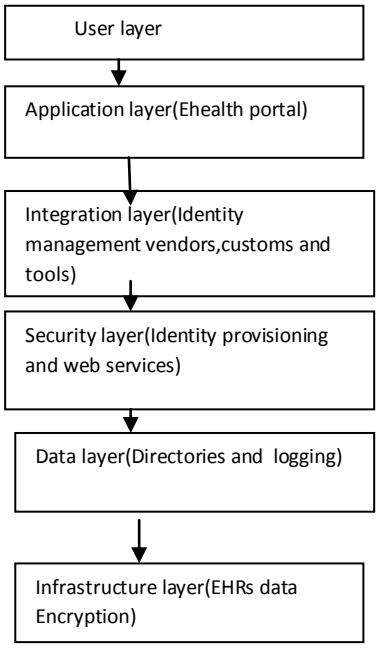

Figure 1 Components of IAM inEhealth system

The system should protect EHRs data and the information produced from the data from having its confidentiality, integrity and availability violated on any layer. The proposed architecture for e-Health system is a practical and exact solution for access control on encrypted EHR data. Managing user's identity and providing adequate privacy and protection in the Ehealth is a great challenge because most providers are depending on different information systems to provide their services.Access controls are known to be the security features that control how users and systems communicate and interact [3][4].Access control can be achieved by ABE. [5]Sahai and Waters proposed an attribute based encryption scheme in 2005. In 2006, Goyal et al. proposed a key-policy attribute based encryption (KP-ABE) scheme [6] that built access policy into the user's private key and described the encrypted data with user's attributes. Ostrovsky et al. proposed a non-monotonic access structure [7] in 2007, and this scheme can let each attribute attach primed word in front of them. And Bethencourt et al. also proposed anciphertext-policy attribute based (CP-ABE) scheme [8] in the same year, and the CP-ABE scheme built the access policy into the encrypted data; a set of attributes is in an user's key. The CP-ABE scheme addresses the problem of KP-ABE that data owner only trusts the key issuer. After that, several schemes were proposed based on the CP-ABE scheme [8, 9].Vimercati et al [10] proposed a solution for securing data storage on untrusted servers using key derivation methods [11].

2.Related Works

The requirements for storage and continuous availability of e-Health data necessitate the use of the cloud computing services [12].Migration of patient health records to the cloud storage relieves the healthcare providers from the infrastructure management tasks [13], [14].In order to achieve the security in ehealth, Identity management and access control mechanisms are enabled to provide authentication and authorization to the EHRs and encapsulations for it. The Identity, Credential, and Access Management (ICAM) Subcommittee, which is responsible for identity management activities of the US government, has adopted a SAML 2.0 profile which is called ICAM SAML 2.0 Web Browser SSO Profile for supporting and managing proper identity authentication during electronic transactions[15]. IAM (Identity and Access management) can also be considered as the first layer of defence in cloud security. A cloud provider used IAM to (i) validate claimed user by verifying the user'scredentials against a directory, and (ii) allow thecustomers to manage identities and authorizations to the resources of customers that are hosted bythe vendor [16]. Users accessing (ehealth) cloud services have three features of IAM - Authorization, Authentication, and Auditing (AAA).Access controls are known to be the security features that control how users and systems communicate and interact [3]. To protect the confidential medical information in cloud, encryption is used. The traditional method of encrypting data has another drawback that data can be selectively shared only at a coarse-grained level [17]. When data is encrypted at fine grained level ABE (Attribute based Encryption) is used. In ABE a sender can encrypt a message specifying an attribute set and a number *d*, such that only a recipient with at least *d* of the given attributes can decrypt the message [18]. ABE enables a user to share the encrypted records among the selected users. To handle the key management challenge the users in the system are conceptually divided into two types of domains labelled as public and personal domains [19].

Preliminaries

The ABE is classified as KP-ABE(Key Policy Attribute Encryption) and CP-ABE (Cipher text Policy Attribute based Encryption).In ABE, the access control decision is based on a set of attributes and the concept of access structure is described as follows

Unique attributes set

(U) is the set of all attributes that describe data properties, user properties and environment properties.

Access structure

In figure 2, an example of an access tree is given which is derived from the following logical expression :((specialty=surgeon AND (division=general surgery OR general surgery = pulmonary) OR (general surgery = anatomy AND (specialty= nurse OR specialty=physician))). This expression means that data can be accessed by all surgeons working in general surgery, pulmonary or anatomy divisions, as well as all nurses working in anatomy division have access.

To understand the basics in this architecture CP-ABE(Cipher text policy attribute based encryption) is necessary since it has more advantage than KP-ABE(Key-Policy attribute based encryption). Ciphertexts can only be decrypted by users who possess all attributes required to satisfy the access policy. Decryption is performed by using secret attribute keys; one such attribute key corresponds to one attribute of a user. Thus, only a user who possesses the right number and combination of these secret keys is able to access the data.

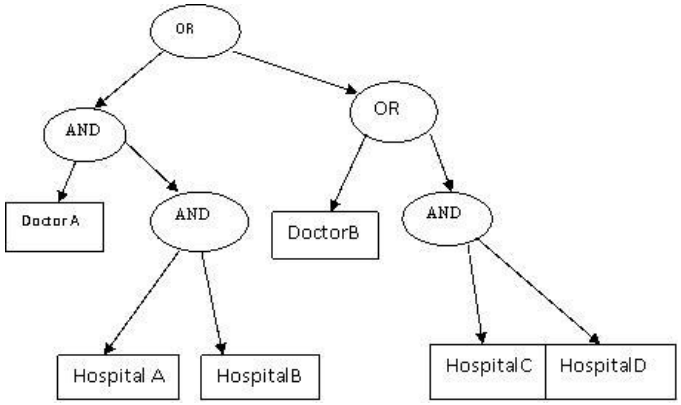

Figure 2An access tree structure

The main construction of CP-ABE scheme consists of four fundamental algorithms:setup, encrypt, key generation, and decrypt**.**In our scheme **decryption** is done in two stagesdecryption I& II.

1.Setup (k): On input of the security parameter*k*, thealgorithm generates a group G_0 of prime order pwith a generator *g* and a bilinear map $\hat{e}$: $G_0 \times G_0 \rightarrow G_1$. The algorithm generates the system attribute set $\psi=(a_1, a_2,.., a_n)$, for some integer m, and for each $a_j \varepsilon \psi$chooses a random elements $t_j \varepsilon Z_p$. Let $y = \hat{e}(g, g)^{\alpha}$, where αis chosen at random from Z_p, and $\{T_j = g^{t_j}\}_{j=1}^{n}$
The public key is published as: $P_k = (g, y, \{T_j\}_{j=1}^{n})$
The master secret key consists of the following components: $M_k = (\alpha, \{t_j\}_{j=1}^{n})$

2. Keygen(M_k , μ, I_u) : To generate a secret key for the userwith an attribute set μand an identifier I_u, the Keygen algorithm performs as follows:
(a) Compute the essential component of the secret key: $d_0 = g^{\alpha - uid}$ where$u_{id} \varepsilon RZ_p$(for each user with an identifier I_ua unique random value $u_{id}$is generated).
(b)Computethe attribute component of the secret key.For each attribute $a_j \varepsilon$ μ, choose $u_{id} \varepsilon RZ_p$and compute $d_{j,1} = g^{u_j / t_j}$ and $d_{j,2} = g^{(u_{id} - u_j)/t_j}$
The secret key of the form: $S_{k\mu Iu, 1} = \{d_{j,1}\} a_j \varepsilon$ μ delivered to the cloning agent and the secret key of the form: $Sk_{\mu Iu,2} = \{d_0, d_{j,2}\} a_j \varepsilon$ μ delivered to the user.

3. Encrypt (m, τ, pk) : To encrypt a message$M \varepsilon G_1$thealgorithm proceeds as follows:
Select a random element $S \varepsilon Z_p$and compute:
$c_0 = g^s$
$c_1 = m. y^s = m. \hat{e}(g, g)^{\alpha s}$
Set the value of the root node τof to be *s*, mark all nodes as un-assigned, and mark the root node assigned. Recursively, for each assigned non-leafnode, suppose its value is *s*, do the following.
If the symbol is ^ and its child nodes are marked un-assigned, let n be the number of nodes, set the value of each node, except the last one, to be $s_i \varepsilon RZ_p$, and the value of the last node to be $s_n = s - \sum_{i=1}^{n-1} si \bmod p$ (irepresents the index of an attribute in the access tree). Mark this node assigned.
If the symbol is □ , set the values of its child nodes to be*s*. Mark this node assigned. For each leaf attribute $a_{j,i} \varepsilon \tau$, compute $c_{j,i} = T^{si}$ Return the ciphertext$c_\tau = \{\tau, c_0, c_1\{c_{j,i}\} a_{j,i} \varepsilon \tau$

4. Decrypt-I($c\tau$, $Sk_{\mu I1}$, I_i):It is run by the CSP(mediator)whenreceiving the ciphertextc_τ, the recipient I_i firstly chooses thesmallest set $\mu^1 \subseteq \mu$ that mediatorc_τ, μ^1, I_i.The CSP mediator checks the Attribute Revocation List (ARL)satisfies τand forwards to the if any $a_j \varepsilon \mu^1$ is revoked either from system attribute set ψor from the user attribute set μ.
(a) If an attribute is revoked, the mediator returns an error symbol □and does not perform further computations.
(b) If no attribute is revoked, the mediator computes $\hat{c}_\tau$ as follows:

$\hat{c}_\tau = \Pi_{aj \varepsilon \mu^1} \hat{e}(T_{j,} g^{u_j / t_j}) \hat{e}(g, g)^{\sum a_j \varepsilon \mu^1 s_j}$

sends$\hat{c}_\tau$ to the recipient

5. Decrypt II ($\hat{c}_\tau$,$sk_{\mu Ii, 2,}$): It is run by the user who needs todecrypt the data.To decrypt the ciphertext the recipient proceeds as follows:
(a) Compute
$C^{11}\tau = \Pi_{aj \varepsilon \mu^1} \hat{e}(T^{sj}_{j}, g^{u_{id} - u_j / t_j})$
$\Pi_{aj \varepsilon \mu^1} \hat{e}(g^{t_j s}_{i}, g^{u_{id} - u_j / t_j}) \hat{e}(g, g)^{\sum a_j \varepsilon \mu^1 (u_{id} - u_j) s_j}$
(b)Compute
$\hat{e}(c_0, d_\rho), \hat{c}_\tau C^{11}\tau = \hat{e}(g^s, g)^{\alpha - Uid} . \hat{e}(g, g)^{\sum a_j \varepsilon \mu^1 (u_{id} - u_j) s_j} . \hat{e}(g, g)^{\sum a_j \varepsilon \mu^1 u_j s_j}$
$= \hat{e}(g^s, g)^{\alpha - Uid} . \hat{e}(g, g)^{Uids}$
$= \hat{e}(g^s, g^{\alpha})$
(c) return m where
$M = c_1 / \hat{e}(g^s, g^{\alpha})$
$= M. \hat{e}(g, g)^{\alpha s} / \hat{e}(g^s, g^{\alpha})$

3. Proposed framework

The objective of the framework is to provide fine grained secured meta access control to the service requester with proper identity management.Figure1 shows proposedarchitecture whichcontains twosubsystems; one is used to provide the identity management. And the second one is used to ensure the fine grained access control using attribute based encryptions for patients electronic health record(EHR) stored in ehealth.The steps and its actions performed in the proposed architecture are represented in the Table 1.The 7 basicelements in the proposed system are described as

A.Patientis a person has to provide allinformation'sabouthim/her to Ehealth provider(hospital) and they has the responsibilities to create the Electronic health record containing patients details and patients has the sole right to access his/her EHR at any time.

B.Electronic Health Record/object

The aggregate electronic record of health-related information on an individual that is created and gathered cumulatively across more than one health care organization and is managed and consulted by licensed clinicians and staff involved in the individual's health and care.

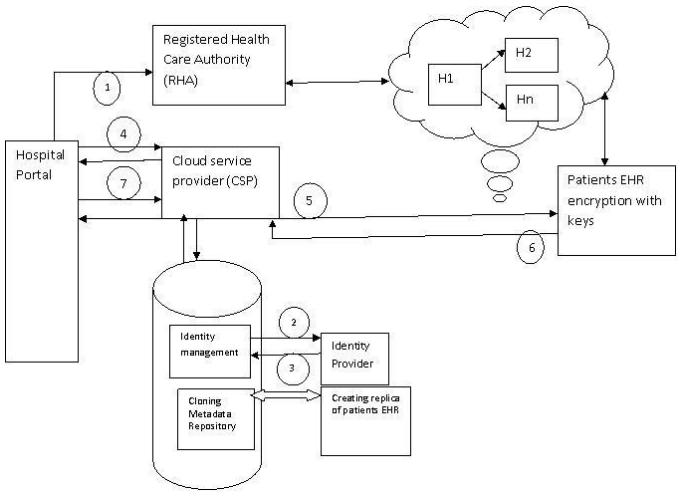

Figure 3 Proposed Architecture

Table 1

Steps	Actions performed
1	Connections from usersin Hospital portal to the RHA(Registered Health Authority)
2	Process of authentication
3	Replication copies of EHR generated
4	Access request from user to CSP
5	CSP checks Access policy constraints
6	Return of access data to the CSP
7	CSP inturn returns access data to users in Hospital Portal

C.Identity managementis to grant safe access to sensitiveinformation and resources to all those who need it, organizations must carefully monitor which users are accessing what resources to ensure that they are accessing the resources that they need in an appropriate manner.

D. Ehealth Cloud generally the cloud is a model for enablingon-demand network access to pool of resources. In ehealth cloud servers all sensitive clinical data about the patient are stored and manipulated and recorded digitally is called as EHR(Electronic Health Record). The EHR stored in the cloud can also be accessed by the patient and users (doctors) from the cloud.

E.Cloning agent The cloning agent is responsible for creatingredundant number of copies of EHRs.It increasesthe speed and time in an efficient manner.

F.User /Subject Users suchas doctors, nurses, are needed toaccess the patients EHR in an essential or an emergency.Thepatients EHR is associated with the set of attributes of the patient.

G.Meta Access Control (MAC) The Access Control is aresolution engine that uses a Meta Access Control model to determine the users that have access right to the EHR/O. The cloning agent is responsible for creating replica of existing patients EHR and send it to Registered Health care authority(RHA), RHA in turn will send this EHR without changing its original configuration to different Hospitals which are registered under RHA in ehealth cloud.The necessity of cloning agent provides faster access to the patients EHR in an emergency situation and shares the secret key. To access the Encrypted EHR of a patient by a physician from one Hospital to another hospital needs the essential attributes.In Meta Access Control subjects are associated with set of attributes of the users and objects /EHRs are associated with policies such as service level agreements which specify how attributes are to be considered for access requests. When a service access request is invoked the policy associated with the requested object is first checked to see whether the requester has the required access or not.If the access is authenticated, policies are checked for additional constraints to approve or deny the access request for authorizing to access. The table 2 shows the components involved in the system to achieve a secured framework.

Table 2

Patient/Person	Electronic health Record	Identity management	Ehealth Cloud	Cloning agent	User/subject	Meta Access control
Public and Master keys generated	Licensed EHR	Grants authentication	Availability of data	Responsibility of redundant data	Secret key generated and shared	Determine authorizat-ion

Process of the framework

The proposed system is composed of the following parties: many users (patients and healthcare professionals like specialist doctors), Ehealth cloudservers, Cloud service providers, cloning agent and the Healthcare Authority (HA) different hospitals connected with Ehealth cloud server. Initiallythe communicationchannels are betweenusers (Doctors), the RHA and cloud servers are secured by a security protocol such as SSL. Once when the patient creates EHR, after authentication of user cloning agent create copies of patients EHR in an encrypted form and send to other health care authorities which is connected with Ehealthcloud. This enhances the system to access the request for availability of

resources in time.In phase I of the proposed work user authentication is processed by identity management using SAML (Security Assertion Mark-up Language).

In phase II itis designedto represent the formal definitions of our proposed scheme andlater give the security model in which our scheme is proven to be secure. We present a scheme for constructing a Cipher text Policy Attribute based Encryption with access policy and provide security under the Decisional Diffie-Hellman assumption. The four algorithms of Cipher text Policy attribute based Encryption (CP-ABE) are executed. RHA from Hospital A has theattributeψ (Hospital A) =a_j.RHA from Hospital B has the attribute ψ (Hospital B) =a_j.Chase [20] gives the construction of the first multi-authority attribute-based encryption (ABE), which allows multiple independent authorities to monitor user attributes. Weextend the idea to use, the essential need is that each RHA could use the function which takes as input I_u and outputs u_{id} requirement thatwe have is that each RHA should use the same function which takes as input$I_u$and outputs u_{id}, where u_{id}*is* used to connect the essential component of thesecret key with the attribute component of the secret key. The component ofthe master secret key $\alpha$is part of the essential component of the secret key but isnot included in the attribute component of the secret keys, therefore, there isno need for attribute authorities to know α. An additional authority is added to control the attributes is Cloud service provider responsible for sharing of the secret keys.And a cloning agent who's is responsible for replication of data.

1.Setup

(a) RHA generates a group G_0 of prime order pwith a generator g and a bilinear map $\hat{e}$: $G_0 \times G_0 \rightarrow G1$. It initializes thecomponent of the master secret key $\alpha \varepsilon RZ_{,\mu^*}$ and the component of the public key $\hat{e}(g, g)^{\alpha\mu}$.Step 1, 2 shows in figure 3

(b) Cloud service provider (CSP)-k*:* Generate the attribute set $\psi_k = (a_k, 1, a_{k,} 2 \ldots a_{k,} m)$.

For each $a_{k,} j\varepsilon\psi_k$set the attribute secret key: $t_k, 1 \ldots t_{k,}$

n, and the attribute public key $\{T_k, j= g^{t_{k,}{}^{j}}\}$

2.Keygeneration

(a) RHA Computes the essential component of the secret key: $d_0 = g^{\alpha\text{-}uid}$

(b) Cloud service provider (CSP-k): Suppose a user with an identifier Iuappliesfor the set of attributes $\mu$to the CSP-k. The CSP kcomputes the attributesecret key as follows: for each $a_{k, j}\varepsilon\mu$, compute $d_{k, j, 1} = g^{uk, j/tk, j}$and $d_{k, j, 2}=g^{(uid\text{-}uk, j)/tk, j}$ where $u_{k, j}\varepsilon R Z_P$.

The RHA is the trusted authority, uses the master key to generate a user secret key, which is then divided into two shares and the first share of the user secret key is sent to the CSP(mediator) and the second share of the user secret key is sent to the user.The mediator has to stay online all the time, while the RHA can be put on-line once it has generated secret keys for all user.

\

IV Security model

In our scheme the RHA is a fully trusted entity which stores securely the master keyand CSP is a semi trusted entity which issues token for decryption to the users. In the security model, the challenger simulates the model and answers adversary queries as follows: gives the public key $P_k$to the adversary .

2. Phase2 model1*:* performs a polynomial bounded number of queries:

Keygen1(μ, Iu)*:* asks for a secret key for the attribute set $\mu$and identifier Iu, and receives the mediator share of the secret key $S_k\mu Iu$, *1*.

Keygen2(μ, Iu)*:* *A* asks for a secret key for the attribute set $\mu$and identifier Iu, and receives the user share of the secret key $S_k\mu Iu$, 2.

3. Challenge*:* sends to the challenger two messages m_0, m_1, and the challengeaccess policy τ^*, such that none of the full secret keys $S_k\mu Iu$(both $S_k\mu Iu$, 1 and$S_k\mu Iu$, 2) generated from the interaction with Keygen1 and Keygen2 oraclessatisfiesτ^*.

The challenger picks a random bit $b\varepsilon(0, 1)$ and returns c_{τ^*}=Encrypt (mb, $_{\tau^*,}P_k$).

Phase2 model2*:* can continue querying with the restriction that none of the full secret keys skμIugenerated from the interaction with Keygen1 and Keygen2satisfies$_{\tau^*}$.

4. Guess*:* outputs a guess $b^1\varepsilon(0, 1)$.

Definition 1.The proposed CP-ABE scheme is said to be semantically secure if any polynomial-time adversary has only a negligible advantage in the security model,where the advantageis defined to be $|Pr[b^1= b]-\frac{1}{2}|$.

Peter is travelling on a vacation. He regularly visits his family doctor working in a Hospital at Mumbai (aka Hospital A). His medical history is stored and digitally maintained in Hospital A which is connected to e-healthcare cloud. During his travel he met with an accident and suddenly got massive heart attack. Neighbor's admitted him to a hospital in Bangalore (aka Hospital B), which is also connected with ehealthcloud. In such a scenario, doctors in Hospital B face several challenges including the access to medical history such as treatments undergone, Medications, previous surgeries if any, drug allergy and the like. In the EMR (emergency) department of (Hospital B) the duty doctor attends this case and provide the first aid treatment. Based on the current status of Peter they analyzed that he was a heart patient, and needs to undergo a bypass surgery immediately. Further hospital B finds the patients information with the identification details available. To proceed for the surgical treatment the doctor in hospital B who is attending this particular patient needs his old history. As both Hospitals are connected to e e-healthcare cloud (private Cloud), system helps in keeping track his Electronic health Record in the cloud in an encrypted form. Now hospital (B) can access the particular patients EHRs through **authentication and authorization process governed by the identity management and fine grained access for the encrypted data in cloud shown in Figure 3** to perform theemergency surgery for the patient.

Security Analysis

A brief discussion about the security of the proposed scheme is reviewed. To decrypt a ciphertext without satisfying the access policy, the adversary has to construct $\hat{e}(g^s g^{\alpha})$, and then divide c1 with $\hat{e}(g^s, g^{\alpha})$ to obtain *M*. To obtain $\hat{e}(g^s, g^{\alpha})$, the adversary must first obtain $\hat{e}(g^s, g^{\alpha})^{suiu}$, which can be calculated by pairing the components of the secret key $g^{uid_i\text{-}uj/\,tj}$ with the components of the ciphertext g^{tjsi}, and then multiply the result with the decryption token $\hat{e}(g, g)^{\Sigma a_j \varepsilon \mu^{1u}{}_j s_j}$ received from the mediator. However, $\hat{e}(g,g)^{suid}$ can be computed only if the adversary has enough attributes which satisfy the access policy, otherwise this would not be possible. If we assume that the adversary is able to compromise the mediator, then the adversary will be able to learn the mediator share of user secret key sk μ Iu, 1, and be able to compute the decryption token $\hat{e}(g, g)^{\Sigma a_j \varepsilon \mu^{1u}{}_j s_j}$. But, the decryption token will not help the adversary to decrypt ciphertext which are satisfied by a set of attributes μ. The reason is because the adversary does not know the second share of the user secret key sk μ I, 2.The very important security of CP-ABE scheme used here is a collusion resistance of user secret keys-it should not be possible for different users to combine their secret keys in order to extend their decryption power. Therefore, to prevent collusion, the Keygen algorithm generates a random value uidforeach user, which is embedded in each component of the user secret key. Users cannot combine components of the secret key since different users have different random value in their secret keys.

V Prototype Implementation

Experimental setup

Eucalyptus 3.4.1 FastStart an open source cloud infrastructure was setup that includes Cloud Controller (CLC), Walrus, Cluster Controller (CC), Storage Controller (SC), Node Controller (NC) configuration, the CLC, Walrus, CC, and SC are installed on one machine, called the Frontend. The NC is installed on another machine, called the Node. In our configuration we have one Frontend and one node.In the Eucalyptus 3.4.1 FastStartconfiguration; all components are installed on one machine. Installing FastStart in the Cloud-in-a-box configuration requires a minimum of 200GB of disk space, a minimum of 4GB of memory and one ethernet NIC. We used a static IP address for Front end and a range of a viable public IP addresses. Eucalyptus will assign these IP addresses to VM Instances. Net beans (version 6.8) platform has been installed to front end used for java based implementation of our proposed authentication scheme.

Case Scenario Consider **a**person when travelled to foreigncountry on his work met with an accident and suddenly he got massive heart attack.Neighbor's admitted this patient to an hospital, where that hospital(A) is connected with ehealth cloud.In the EMR(emergency) department the duty doctor attends this case and provide the first aid treatment and finds the patients personal information with the ID card.They then analyzed that the patient was a heart patient needs to undergo a surgery immediately since of the accident he met. To proceed for the surgical treatment the doctor in hospitalA who is attending this particular patient needs his old history. Previously the patient was regularly visiting a specialist in another hospital(B) which is also connected with ehealth cloud.Ehealth is a system which keeps track of all patients Electronic health Record in the cloud in an encrypted form.

Now the doctor from hospital (A) can access the particular patients EHRs through authentication and authorization process governed by the identity management and fine grained access for the encrypted data in cloud and proceed with doctor's team in hospital to do the emergency surgery for the patient.

VI Conclusion

We considered a new approach as cloning agent to publish the encrypted files to different authorities of different organizations for fast retrieval and availability of data in an emergency.Along with the CPABE an additional effort is added to split the secret key to share to the users to secure the data stored in cloud.A flexible control of encrypted data stored in cloud is provided and fine grained access control is attained with fast decryption.In future work, this system is going to integrate more web-based services to promote the functionalities and the capabilities to make vital service in EHealth cloud.

References

[1] Tim, Subra, Shahed, 2009, Cloud Security and Privacy, United States :1st ed.

[2] Devki Gaurav Pal, Ravi Krishna, Prashant Srivastava, Sushil Kumar, Monark Bag, Vrijendra Singh, June 2012, "A Novel Open Security Framework for Cloud Computing ", India International Journal of Cloud Computing and Services Science Vol.1, No.2, pp. 45-52.

[3] Noemi Antedomenico, December 2010, "Optimizing security of cloud computing within the DoD, "Thesis, Naval PostGraduateSchool, Monterey, california.

[4] Steffen Schreiner, April 2009, "The Impact of Linux Superuser Privileges on System and Data Security within a Cloud Computing Storage Architecture", Thesis, TechnischeUniversität Darmstadt.

[5] Cheng-Chi Lee[1], Pei-Shan Chung[2], and Min-Shiang Hwang[3], July 2013, "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments, International Journal of Network Security, Vol.15, No.4, PP.231-240.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 2006, "Attribute-based encryption for fine-grained access control of encrypted data, ", Proceedings of the 13th ACM conference on Computer and communications security, pp. 89-98.

[7] R. Ostrovsky, A. Sahai, and B. Waters, 2007, "Attribute based encryption with non-monotonic access structures, ", Proceedings of the 14th ACM conference on Computer and communications security, pp. 195-203.

[8] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, 2010, "Fully secure functional encryption:Attribute-based encryption and hierarchical) inner product encryption, " Advances in Cryptology V EUROCRYPT, vol. 6110 of LNCS, pp. 62-91.

[9] B. Waters, 2011, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, " Public Key Cryptography V PKC, vol. 6571 of LNCS, pp. 53-70.

[10] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, 2007, "Over-encryption: Management of access control evolution on outsourced data", Proceedings of VLDB.

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, 2005, "Improved proxy re-encryption schemes with applications to secure distributed storage", Proceedings of NDSS.

[12] S. P. Ahuja, S. Mani, and J. Zambrano, September 2012 "A survey of the state of cloud computing in healthcare, " Network and Communication Technologies, Vol. 1, No. 2, pp. 12-19. [13]S. Yu, C. Wang, K. Ren, and W. Lou, March 2010, "Achieving secure, scalable and fine-grained data access control in cloud computing, " IEEE INFOCOM Proceedings, pp. 1-9.

[14] B. Horowitz, December 20, 2012, Cloud Computing Brings Challenges for Health Care Data Storage, Privacy.

[15] Federal Identity, 16-Dec-2011, "Security Assertion Markup Language (SAML) 2.0 Web Browser Single Sign-on (SSO) Profile", Credentialing, and Access Management.

[16] Manny Siddiqui, Spring 2011, "Cloud Computing Security", Paper Blog, INFO 661.

[17] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, 2009, "Patient controlled encryption: ensuring privacy of electronic medical records", Proceeedingsof CCSW '09, pp. 103-114.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, 2006, "Attributebased encryption for fine-grained access control of encrypted data", Proceedings of CCS '06, pp. 89-98.

[19] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, 2012, " Scalable and Secure Sharing of Personal Health Records inCloud Computing using Attribute-based Encryption", IEEE Transactions on Parallel and distributed systems, vol.xx, No.xx.

[20] M. Chase, 2007, Multi-authority Attribute Based Encryption. In *Theory of Cryptography*, Springer, volume 4392, pages 515-534.