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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

Secure Patient-Centric Frame Work In Cloud Computing Using Attribute Based Encryption

M.Sreenadh[1], S.Kusuma[2]

M. Tech (CSE), MITS, Madanapalle, A.P, India[1]

Assistant Professor (CSE Dept), MITS, Madanapalle, A.P, India[2]

Abstract: Personal health record (PHR) is associate degree rising patient-centric model of health info exchange, th at is usually outsourced to be hold on at a 3rd party, like cloud suppliers. However, there are wide privacy considerations as personal health info might be exposed to those third party servers and to unauthorized parties. To assure the patients' management over access to their own PHRs, it\'s a promising technique to inscribe the PHRs before outsourcing. Yet, problems like risks of privacy exposure, measurability in key management, Easy access and user Interaction made simple, have remained the foremost necessary challenges toward achieving fine-grained, cryptographically implemented information access management. During this paper, we have a tendency to propose a unique patient-centric framework and a collection of mechanisms for information access management to PHRs hold on in semi-trusted servers. To realize fine-grained and climbable information access management for PHRs, we have a tendency to leverage attribute primarily based encoding (ABE) techniques to inscribe every patient's PHR file. Totally different from previous works in secure information outsourcing, we have a tendency to concentrate on the multiple information owner state of affairs, and divide the users within the PHR system into multiple security domains that greatly reduces the key management complexness for homeowners and users. A high degree of patient privacy is warranted at the same time by exploiting multi-authority ABE. Our theme additionally permits dynamic modification of access policies or file features, provides finest demanding needs for user/attribute revocation and break-glass access underneath emergency situations. Intensive analytical and experimental results area unit given that show the safety, measurability and efficiency of our planned theme.

Index Terms: Personal health account, cloud computing, data privacy, fine-grained right to use control, characteristic-based encryption

I. INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health data exchange. A PHR service permits a patient to form, manage, and management her personal health information in one place through the net, that has created the storage, retrieval, and sharing of the medical data a lot of efficient. Especially, every patient is secure the total control of her medical records and might share her health data with a good vary of users, together with care providers, relations or friends. As a result of the high cost of building and maintaining specialized information centers, Many PHR services are outsourced to or provided by third-party service suppliers, as an example, Microsoft HealthVaule1. Recently, architectures of storing PHRs in cloud computing are planned in [2], [3].

While it's exciting to possess convenient PHR services for everybody, there are units several security and privacy risks which may impede its wide adoption. The most concern is regarding whether or not the patients may truly management of their sensitive personal health data (PHI) the sharing, particularly once they area unit hold on a third-party server which individuals might not totally trust. On the one hand, though there exist care rules such as HIPAA that is recently amended to include Business associates [4], cloud suppliers area unit typically not covered entities [5]. On the opposite hand, attributable to the high value of the sensitive personal health data (PHI), the third-party storage servers area unit usually the targets of various malicious behaviors which can result in exposure of the PHI. As a renowned incident, a Department of Veterans Affairs info containing sensitive alphabetic character of 26.5 million military veterans, as well as their social security numbers And health issues was taken by an employee WHO took the information home while not authorization [6]. To confirm patient-centric privacy management over their Own PHRs, it's essential to possess fine-grained information access control mechanisms that employment with semi-trusted servers. A possible and promising approach would be to inscribe the data before it is given as source. Actually, the PHR owner herself ought to decide a way to inscribe her files and to allow that set of users to get access to every file. A PHR file ought to solely be offered to the users WHO area unit given the corresponding decipherment key, whereas stay confidential to the remainder of users. Moreover, the patient shall

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

continuously retain the proper to not solely grant, but also revoke access privileges once they feel its necessary [7].

However, the goal of patient-centric privacy is commonly in conflict with quantifiability in a very PHR system. The approved users might either got to access the PHR for private use or skilled functions. Samples of the previous are loved one and friends, whereas the latter will be checkup doctor's office, pharmacists, and researchers, etc.? We refer to the 2 classes of users as personal and skilled users, severally. The latter has doubtless massive scale; ought to every owner herself be directly accountable for managing all the skilled users, she is going to simply be powerless by the managing key is difficult. User's access requests area unit typically unpredictable, it's tough for AN owner to work out a list of them. On the opposite hand, completely different from the only data owner situation thought of in most of the prevailing works [8], [9], in a very PHR system, there are a unit multiple homeowners who might inscribe in step with their own ways that, possibly using completely different sets of scientific discipline keys. Lease every user get keys from each owner whose PHR she wants to scan would limit the accessibility since patients are not continuously on-line. an alternate is to use a central authority (CA) to try and do the key management on behalf of all PHR homeowners, however this needs an excessive amount of trust on one authority (i.e., cause the key written agreement problem).

In this paper, we tend to endeavor to check the patient centric, secure sharing of PHRs hold on semi-trusted servers, and specialize in addressing the sophisticated and challenging key management problems. So as to safeguard the personal health information hold on a semi-trusted server, we adopt attribute-based secret writing (ABE) because the main encryption primitive. Using ABE, access policies area unit expressed supported the attributes of users or their info, which enables a patient to by selection share her PHR among a set of users by encrypting the file underneath a collection of attributes, while not the necessity to grasp an entire list of users. The complexities per secret writing, key generation and decipherment area unit solely linear with the quantity of attributes concerned. However, to integrate ABE into a large-scale PHR system, vital problems like key management quantifiability, dynamic policy updates, and efficient on-demand revocation area unit non-trivial to unravel, and stay mostly open up-to-date. To the current finish, we make the subsequent main contributions:

(1) We tend to propose a completely unique ABE-based framework for sharing of PHRs in cloud computing with patient centric environments by providing security, underneath the settings of multi user. To address the key management challenges, we tend to conceptually divide the users within the system into 2 sorts of domains, namely public and private domains. Particularly, the bulk professional user's area unit managed distributive by attribute authorities within the former, whereas every owner solely needs to manage the keys of a tiny low variety of users in her personal domain. During this means, our framework will simultaneously handle differing types of PHR sharing applications' necessities, whereas acquisition bottom key management overhead for each homeowners and users within the system. Additionally, the framework enforces write access control, handles dynamic policy status, and implies break-glass access to PHRs underneath emergence situations.

(2) Within the property right, we tend to use multi-authority ABE (MA-ABE) to boost the protection and avoid key written agreement problem. Every attribute authority (AA) in it governs a disjoint set of user role attributes, whereas none of them alone is ready to manage the protection of the complete system. We tend to propose mechanisms for key distribution and secret writing so PHR homeowners will specify personalized fine-grained role-based access policies throughout file secret writing. Within the personal domain, homeowners directly assign access privileges for private users and inscribe a PHR file underneath its information attributes. Moreover, we enhance MA-ABE by asserting AN economical and on-demand user/attribute revocation theme, and prove its security underneath normal security analysis. In this way, patients have full privacy management over their PHRs.

(3) We offer a radical analysis of the complexness and quantifiability of our planned secure PHR for solution of sharing, in case of multiple attributes in computation, communication, storage and managing the keys. We also compare our theme to many previous ones in complexity, quantifiability and Confidentiality. However, we demonstrate the potency of our theme by implementing it on a contemporary digital computer and activity experiments/simulations. There are units many main further contributions:

(1) We clarify and extend our usage of MA-ABE within the public domain, and formally show however and that varieties of user-defined file access policies area unit complete.
(2) We clarify the planned revocable MA-ABE theme, and provide a proper security proof for it.
(3) We feature out both real-world experiments and simulations to gauge the performance of the planned answer during this paper.

II. BACKGROUND

On twenty nine Gregorian calendar month 2011, in his fall disbursal Review, the Chancellor of the monetary resource announced: 'The Government can guarantee all NHS

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

patients will access their personal doc records on-line by the top of this Parliament.' Patients having access to their own records on-line (referred to as 'Record Access') is recognized as Associate in Nursing early step towards patients managing their own 'Personal Health Record' (PHR).

For the needs of this survey results, use the Markle Foundation's definition of a PHR, is given as:

'An Internet-based set of tools that enable individuals to access and coordinate their womb-to-tomb health info and build applicable parts of it accessible to people who would like it.' (During our analysis, we have a tendency to found several varied definitions of Personal Health Records, summarized in Appendix A, which additionally includes a wordbook of terms.)

The barriers to delivery regarding on-line patient access to their health records square measure vital. as an example, public understanding of the social also as clinical edges of Record Access desires promoting if demand is to be stimulated by patients. We have written this report in order that policy manufacturers, clinicians, patients and people in health science might gain bigger insight to the controversy regarding the advantages of Record Access and PHRs. we have a tendency to initial explore the background and policy drive towards Record Access, and then think about more steps to make sure patients get the foremost from the system. We have a tendency to additionally explore the need of patients to adopt and use PHRs and what styles of patients would be most impelled to use them.

This report is predicated on surveys, supplemented by a comprehensive review of the proof around relevant developments each within the Britain and abroad, and with consideration of people's on-line usage with different sectors and services. We have a tendency to additionally draw on case studies and examples maybe progress and problems. In specializing in the angle of the user, the survey does not address wider however crucial problems arising from increased patient use of PHRs, such as: the impact on clinical apply and culture; the organization of care; the business case; security and Authentication; or the implementation problems related to delivery PHRs into use. Moreover, we have a tendency to don\'t touch upon specific PHR products however draw on case studies from a spread of supplier's maybe their use. 2020health's work was undertaken throughout the spring of 2012. It had been created attainable by Associate in nursing unrestricted instructional grant from Microsoft, UN agency additionally supported the Patient Information Forum's 'Guide to Health Records Access', published earlier within the summer.

Personal health records must first be own:

Remember seeing photos of what the primary cars looked like? They looked a bit like carriages, however while not the horses. It took years to evolve far away from the idea of simply swing associate engine on a carriage. For advocates of health data computing, PHR Design is making an attempt to assist North American country leap over all of the years of building larger, horseless buggies and suppose instead about the way to build a good installation. PHR Design is rethinking current ideas of what personal health records will and will be before ideas become implemented and policies to control the restricted visions are established. Instead of simply read PHRs as inactive repositories of data, PHR Design challenges all folks to form PHRs that are extremely tailored to assist shoppers meet their specific health care desires and supply a record of data that's vital to patients and their doctors. That's exciting. And for the healthcare sector, it's also revolutionary because establishments and clinicians mainly suppose what general data they need available to present patients, not what specific data patients may wish and want to understand to enhance their regular lives and manage their own health.

I think it's clear to several folks that the PHRs being developed these days don't seem to be as helpful as they have to be if each folks goes to use them to require charge of our own health and health care. That's as a result of presently available PHRs don't seem to be terribly personal and they cannot be bespoke fine. Many folks suppose PHRs supply us a valuable service if they {let North American country allow us to} go surfing to check all of our own clinical knowledge in one place and that's true. But what can we have a tendency to do with this information? However will we have a tendency to use it to help North American country improve our own health? That's the challenge PHR Design aims to unravel. Take fleshiness, for instance. It's one among the best issues of American society these days, however no PHR as presently envisioned are ideal for serving to patients turn. PHRs of the long run, the sort that PHR design hopes to spark, might daily prompt someone to induced in his or her own health care creating a meal and exercise arrange that's right for his or her explicit needs, chase progress over time and sharing data with his or her doctor in an exceedingly timely fashion.

Technology designers and policy-makers ought to inspect the technical features like cell phones and social networks on the net and rethink however they'll be used to manage our health as a part of a broader PHR framework. When PHR Design concludes, we will have one or two of solid, operating prototypes that demonstrate innovative approaches for a way PHRs will facilitate us drive our own health care selections. We should always additionally have additional folks making PHRs that are far more useful than what

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

several folks have presently visualized. That kind of big-picture thinking is painfully required.

III. RELATEDWORK

For access management of outsourced knowledge, partly trusty servers are usually assumed. With cryptographic techniques, the goal is making an attempt to enforce United Nations agency has (read) access to that components of a patient's PHR documents during a fine-grained means.

A. radial key cryptography (SKC) primarily based solutions: Symmetric-key algorithms are a category of algorithms for cryptography that use an equivalent cryptanalytic keys for both secret writing of plaintext and cryptography of cipher text. The key is also identical or there is also a straight forward transformation to travel between the 2 keys. The keys, in observe, represent a shared secret between 2 or additional parties that can be wont to maintain a personal info link Vimercati et.al. [6] Planned an answer for securing outsourced data on semi-trusted servers supported radial key derivation strategies, which might attain fine-grained access Control. Sadly, the complexities of file creation and user grant/revocation operations are linear to the amount of authorized users that is a smaller amount scalable.

B. Public key cryptography (PKC) primarily based solutions: PKC primarily based solutions were planned because of its ability to separate write and skim privileges. To appreciate fine-grained access management, the normal public key secret writing (PKE) primarily based schemes planned by J. Benaloh, M. Chase, E. Horvitz, and K. Lauter [1] in their work "Patient controlled encryption: making certain privacy of electronic medical records" ,they purpose the answer situation and shows however public and radial primarily based secret writing used , disadvantage of their solution is either incur high key management overhead, or need encrypting multiple copies of a file victimization completely different users' keys.

C. Attribute {based mostly primarily based} secret writing based solutions: A number of works used ABE to appreciate fine-grained access management for outsourced knowledge, especially, there has been associate increasing interest in applying ABE to secure electronic health care records (EHRs). Narayan et al. planned associate attribute-based infrastructure for EHR systems, wherever every patient's EHR files are encrypted employing a broadcast variant of Cipher Text-ABE (CP-ABE) [4] .However, the cipher text length grows linearly with the amount of unrevoked users. In [16], a variant of ABE that permits delegation of access rights is planned for cipher EHRs. Ibraimi et.al. [5] Applied cipher text policy ABE (CP-ABE) [8] to manage the sharing of PHRs, and introduced the thought of social/professional domains however they are doing not use multi-authority ABE. In [3], Akinyele et al. investigated victimization ABE to generate self-protecting EMRs, which might either be hold on cloud servers or cell phones so EMR may be accessed once the health supplier is offline. Disadvantage is device dependency and revocation isn't supported. Other Common disadvantage of all higher than solutions is drawback of key-escrow as they contemplate single trusty authority.

IV. PROPOSED SOLUTION

Personal Health Record Owner:

The PHR owner is registered under the system by providing his Personal Information. When a PHR User Requests for Registration into the server. The user is provided with a Secret Key and a Public Key. The PHR owner can store his data on to the server by using encrypting it by using Key-Policy Attribute Based Encryption. The owners refer to patients who have full control over their own PHR data, i.e., they can create, control and delete it. The Owner can make his data private or Public on his own choice. The private data will be only available to the PHR Owner and it could be Viewed or downloaded only when the Secret Key of associated PHR owner is Submitted to the server. The owner keeps his data as public then the public authority agents like hospitals, insurance companies and the Search users like doctors, physicians can view all the Public data of the PHR system by using their Secret Key. But, the Sensitive data which kept as private is confidential and can't be viewed by any of the other users in the PHR System.

Public Authority Agents (PPAs):

Public Authority Agents (PPAs) can view the data of a PHR Owner which is Public and Personal Information. The PAAs Maintains the Personal Information of a PHR Owner and the users. The PPA can able to send an Secret key to an user who requests for data of a patient(PHR Owner) through Emergency Services using Multi-Authority AttributeBasedEncryption By using that key the user can access the respective PHR owners data for that particular session only. The PPAs has Control over the Public data of PHR. Even though the PPAs has Control over the PHR data, they don't have permission to write or change PHR Owner data. They can view and read only. The PPAs can view the Personal Information of a User, PHR Owner and the Public data of a PHR owner. They can provide temporary access for an emergency Service to access the PHR data of a PHR Owner by using MA-ABE by implementing Break Glass Access.

Search User:

The user is search users like doctors, physicians who are interested to view and research the PHR data available in PHR server. They don't keep any PHR data in the System

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

but interested in accessing the other PHR owner's data and getting Information from them. The User Registers on to the server by providing his Personal information and the user gets a Secret key after registration. By which he can explore the Health Records of Patients (PHR Owners) and can view them by providing his Private Key generated by Generic Anonymous Key Issuing Protocol of MA ABE Which is provided by the PHR server. The user if enters the correct Secret key He can able to view the PHR data. If the User Don't have the correct key and he tries to moles rate by giving the wrong key and try to access a PHR Data. The user is Blocked and not allowed to login to the PHR permanently. If the user gives the valid key then he can able to View the PHR data.

Break-glass:

In Emergency cases, the regular access policies may no longer be appropriate. To handle this situation, break-glass access is needed to access the Respective PHR data of a patient. In our Project, each owner's PHR's access right is also delegated to an emergency department. To prevent from mistreatment of break-glass option, the emergency staff requests to contact the emergency department to verify her identity with the emergency situation, and obtain brief read keys. After the emergency is over, the patient can revoke the emergent access via the emergency department.

On-demand revocation:

Whenever a user's attribute is no longer valid, the user must not be able to access future PHR files using that attribute. This is typically called attribute revocation, and the parallel security property is forward secrecy. There is also user revocation, where all of a user's entrée privileges are revoked. When a user tries to access the PHR Records with incorrect Secret key which do not satisfies the attributes of that Record. The User will be revoked from the PHR.

Algorithms of for KP-ABE with improvement are discussed as below:

1) KP-ABE Setup (A): Outputs public key PK and Master key MK for A as set of attributes Associate for each attribute in A with attributes universe as U = {1, 2... n}. It defines a bilinear group G1 of prime order p with a generator g, a bilinear map e: G1 × G1 -> G2 which has the Properties of bilinearity, computability, and non-degeneracy. Associate each attribute i ∈ U with a number ti and also chose y uniformly at random in Zp* and y.
The public key is:

PK = (T1 = gt1, ..., T1 = gt|U | , Y = e(g, g)y)

The master key is:

MK = (t1,…, t|U |, y)

2) KP-ABE Encryption (M, γ, PK): M message in GT with a set of attributes γ , PK is public Key , outputs
Cipher Text E. Choose a random value s in Zp. Encrypt a secret message M in GT with a set of attributes γ.
The cipher text is: E = (γ, E' = MY s, {Ei = Tis} where i∈ γ)

3) KP-ABE Key Generation (A, MK): This algorithm output a secret key D embedded with an access structure T. The access structure A is realized by the following three steps:

1. For root node r, set value secret = y. mark all node un-assigned and mark root node assigned.
2. Recursively, for each assigned non-leaf node,

a. If the operator is ^ (and) and its child nodes are noticeable un-assigned, let n be the number of child nodes, set the value of each child node, except the last one, to be si ∈ Zp, and the value of the last node to be sn = s -∑ si . Mark this node assigned.

b. If the operator is V (or), set the values of its child nodes to be s. spot this node assigned.

3. For each leaf attribute aj,i ∈ T , compute Dj;i = Tj∧si
Output: Secret Key Sk= { Dj,i}

4) KP-ABE Decryption (E, D) this algorithm takes as input the cipher text E encrypted under the attribute put U, the user's secret key SK for entrée tree T, and the public key PK. Finally it output the message M if and only if U satisfies T.

Basic Algorithm of the MA-ABE with improvement is:

1) Key Issue (Attributes, MK, PK). This algorithm, the AAs together actively generates a secret key for a user. For a user with (secret) ID u, the secret key is in the form:
SKu = ⟨Du = g^Ru ,, {Dk;i = g^(qk(i)/tk,i) , Verk,i} k∈{1…N} ⟩
where Ru is a universal ID for user u, and qk(0) = Σk vk − Ru.

1) KeyIssue(Attributes ,MK, PK). This algorithm, the AAs together actively generates a secret key for a user. For a user with (secret) ID u, the secret key is in the form:
SKu = ⟨Du = g^Ru ,, {Dk;i = g^(qk(i)/tk,i) , Verk,i} k∈{1…N} ⟩
Where Ru is a universal ID for user u, and qk(0) = Σk vk − Ru.

2) Encryption (M, PK, attributes []): This algorithm take a message M, PK and a set of attributes and outputs the cipher text E as follows:
The encryption first chooses an s ∈ Zp, and then returns:

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

CT = [E0 = M·Y^ s,E1 = g2^s, {Ck;i = Tk;i^s, Verk;i};k∈{1..N}]
where i= no of attributes form power k

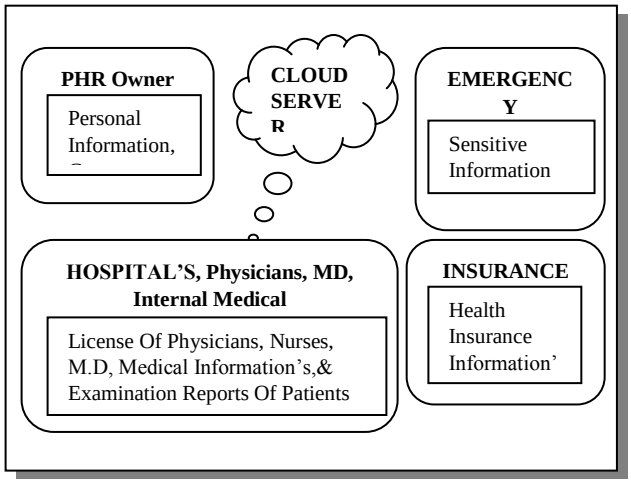
3) Decryption (CT, SKu): This algorithm takes as input a cipher text CT and a user secret key SKu. If for each AA k,
If the version of attribute in SK and CT match, algorithm pairs up Dk;i and Ck;i and reconstructs e(g1, g2)^sqk(0). After multiplying all these values together with e(Du,E1), u recovers the blind factor Y ^ s and thus gets M.

4) Update Parameter: This algorithm updates an attribute to a new description by redefining its system master key and Public key component. It also outputs a proxy re-encryption key and re-secret-key between the old description and the new description of the attribute.

5) UpadteSecretKey: This algorithm translates the secret key element of attribute i in the user secret key SK from an old description into the latest description using re-secret-key generated in step 4.

6) ReEncryptFile: This algorithm translates the cipher text element of an attribute i of a file from an old description into the latest version using proxy- encryption key generated in step 4.

BLOCK DIAGRAM



IMPLEMENTATION

In this Paper implantation details of paper a unique framework of secure sharing of private medical records in cloud computing.

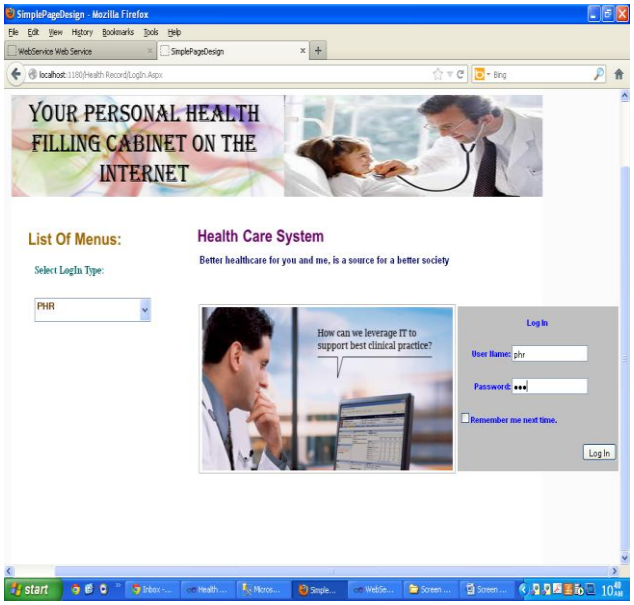
Home Page:
The Home Page is necessary for any website likewise this website is also having the Home Page this home page gives total information about this website like.,

- Home Page
- Feedback
- About us
- Contact us

This home page is also having the log in process.

Log In:

You can only login to your account if you have your Email/Username and password. Please keep login information in a safe place. If you lose it, you will not be able to login to your account.

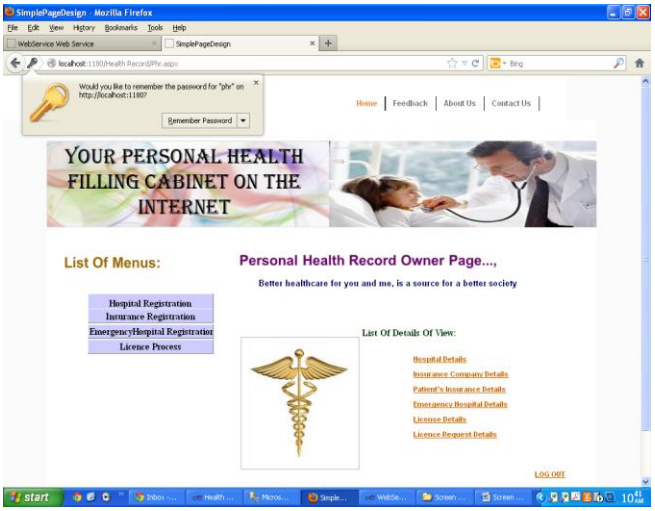


ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 10, October 2013

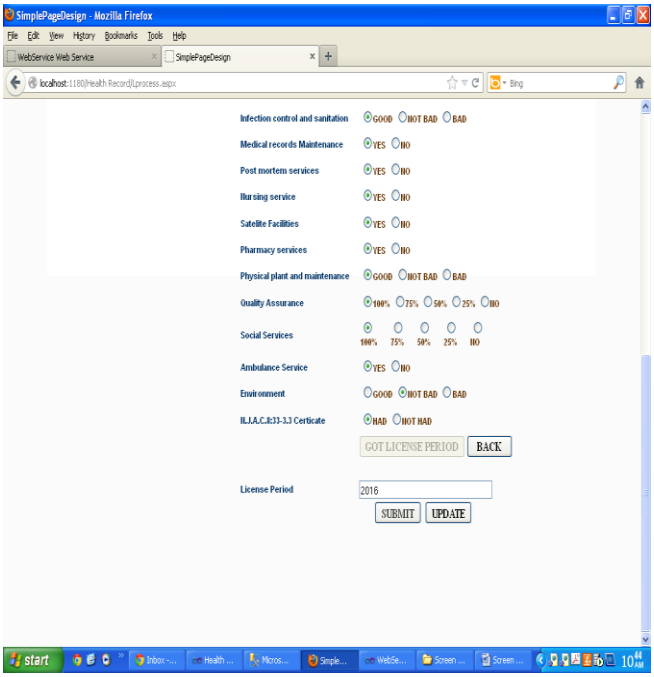
PHR Owner:

The PHR owner is registered under the system by providing his personal information. When a PHR user requests for registration into the server. The user is provided with a secret key and public key. The PHR owner can store his data on the server by using the encrypting it by using key-policy Attribute Based Encryption.
The PHR owners refer to patients we have full control over their own PHR Data, they can Create, control, manage and delete it. The owner can make his data private or public on his own choice.



License Process:

Every hospital and Doctors having their own license. Our PHR owner verify that license details and passport verification for getting authorized doctor. If the license will be in expired the PHR owner notifies that particular hospital or doctor for license renewal.



V. CONCLUSION

In this Paper, we've conferred the detail style and Implementation detail of projected a unique framework of secure sharing of private medical records in cloud computing. Considering part trustworthy cloud servers, we argue that to completely understand the patient-centric conception, patients shall have complete management of their own privacy through encrypting their anamnesis files to permit fine-grained access. The framework addresses the distinctive challenges brought by multiple house owners and users, therein we tend to greatly scale back the complexness of key management whereas ensured the privacy. we tend to utilize numerous varieties of ABE to write in code the anamnesis files, so patients will permit access not solely by personal users, however conjointly numerous users from public domains with totally different skilled roles, qualifications and affiliations.

REFERENCES

[1]. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW '09, 2009, pp. 103–114.
[2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.
[3]. A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin. Self-protecting electronic medical records using attribute-based encryption on mobile device. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010. http://eprint. iacr. Org/2010/565.
[4]. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

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

[5]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
[6]. *S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati*, "Over-encryption: management of access control evolution on outsourced data," in VLDB '07, 2007, pp. 123–134.
[7]. A. Sahai and B. Waters. Fuzzy identity-based encryption. Advances in Cryptology {EUROCRYPT 2005, pages 457{473, 2005.
[8]. *Angelo De Caro and Vincenzo Iovino*, "jPBC: Java Pairing Based Cryptography" Computers and Communications (ISCC), 2011 IEEE Symposium on Digital Object Identifier: 10.1109/ISCC.2011.5983948 Publication Year: 2011, Page(s): 850 – 855
[9]. *M. Chase and S. S. Chow*, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp. 121–130.

BIOGARPHIES

M. Sreenah was born in Andhra Pradesh, India, in 1989. He received the bachelor degree, B.Tech (CSIT) from the University of JNTU, Hyderabad, in 2011. He is currently pursuing Master degree, M.Tech (CSE) in Madanapalle Institute of Technology & Science, Madanapalle.

S. Kusuma received B.E (CSIT) from R.L. jalappa Istitute of Technology, Bangalore and M.Tech (CSE) from the University of JNTU Ananthapur, Madanapalle. She is currently working as Assistant Professor, Department of CSE in Madanapalle Institute of Technology & Science. Madanapalle.