ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

User Revocation And Fine Grained Access Control Of Phr In Cloud Using Hasbe

T.Radhika[1], S.Vasumathi Kannagi[2]

P.G.Scholar, Department of CSE, Info Institute of Engineering, Coimbatore, India[1]

Assistant Professor, Department of CSE, Info Institute of Engineering, Coimbatore, India[2]

ABSTRACT: Cloud computing has emerged as one of the most influential paradigms in the IT industry in recent years. Since this new computing technology requires users to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. Several schemes employing Attribute-Based Encryption (ABE) have been proposed for access control of outsourced data in cloud computing, however, most of them suffer from inflexibility in implementing complex access control policies. The proposed scheme used is Hierarchical Attribute-Set-based encryption by extending cipher text-policy Attribute-Set-Based Encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE. In addition, ASBE employs multiple value assignments for access expiration time to deal with user revocation more efficiently than existing schemes. We formally prove the security of HASBE based on security of the Cipher text-Policy Attribute-Based Encryption (CP-ABE) scheme and analyze its performance and computational complexity. We introduced the ASBE scheme for realizing scalable, flexible, and fine-grained access control in cloud computing. The ASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. ASBE not only supports compound attributes due to flexible attribute set combinations, but also achieves efficient user revocation because of multiple value assignments of attributes.

KEY WORDS: HASBE, cloud computing, personal health records, fine-grained access control

I. INTRODUCTION

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. Shucheng Yu et.al[1]have proposed Achieving Secure, Scalable, And Fine-Grained Data Access Control In Cloud Computing enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. We achieve our design goals by exploiting a novel cryptographic primitive, namely key policy attribute-based encryption (KP-ABE) and uniquely combine it with the technique of proxy re-encryption (PRE) and lazy re-encryption. User secret keys are defined to reflect their access structures so that a user is able to decrypt a ciphertext if and only if the data file attributes satisfy his access structure. Such a design also brings about the efficiency benefit, as compared to previous works, in that, the complexity of encryption is just related the number of attributes associated to the data file, and is independent to the number of users in the system; and data file creation/deletion and new user grant operations just affect current file/user without involving system-wide data file update or re-keying. One extremely challenging issue with this design is the implementation of user revocation, which would inevitably require re-encryption of data files accessible to the leaving user, and may need update of secret keys for all the remaining users. Cong Wang et.al [2] have proposed attribute based data sharing with attribute revocation for IBE, which is also applicable to KP-ABE and fuzzy IBE. Ming Li et.al [3] have proposed authorized private keyword search over encrypted personal health records in cloud computing is a fine-grained authorization framework in which every user obtain search capabilities under the authorization of local trusted authorities (LTAs), based on checking for user's attributes. The central TA's task is reduced to minimum, and can remain semi-offline after initialization. Using an obtained capability, a user can let the cloud server search through all owners' encrypted PHRs to find the records that match with the query conditions. Our framework enjoys a high level of system scalability for PHR applications in the public domain. Josh Benaloh et.al [4] have proposed patient controlled encryption: ensuring privacy of electronic medical records refer to as Patient Controlled Encryption (PCE) as a solution to secure and private storage of patients' medical records. PCE allows the patient to selectively share records among doctors and healthcare providers. The design of the system is based on a hierarchical encryption system. The patient's record is partitioned into a hierarchical structure, each portion of which is encrypted with a corresponding key. Ting-Yu et.al [5]have proposed a unified scheme for resource protection in automated trust negotiation in centrally managed security domains. Every entity that can take actions within such a system has one or more identities in that domain. The system grants or denies an entity's requests to access certain resources according to its access control policies and the authenticated identities of the requester. Underlying assumption is that entities in the system already know each other. Amit Sahai et.al [6] have proposed ciphertext-policy attribute-based encryption in which, a user will only be able to decrypt a cipher text if that user's attributes pass through the cipher text's access structure. In this work, we provide the first construction of a cipher text-policy attribute-based encryption (CP-ABE) to address this problem, and give the first construction of such a scheme. In our system, a user's private key will be associated with an arbitrary number of attributes expressed as strings. Kristin Lauter [7]have proposed automated trust negotiation using cryptographic credentials have been developed to address oblivious signature. Brunelli.D [7] have proposed cloud computing and emerging it platforms:vision, hype, and reality for delivering computing as the 5th utility consisting of services that are commoditized and delivered in a manner similar to traditional utilities such as water, electricity, gas, and telephony. In such a model, users access services based on their requirements without regard to where the services are hosted or how they are delivered. Amit Sahai et.al [10] have proposed fuzzy identity-based encryption is a new type of Identity-Based Encryption that we call Fuzzy Identity-Based Encryption in which we view identities as a set of descriptive attributes. In a Fuzzy Identity-Based Encryption scheme, a user with the secret key for the identity is able to decrypt a cipher text encrypted with the public key 0 if and only if and 0 are within a certain distance of each other as judged by some metric. Mrinmoy Barua et.al [11] have proposed principles of policy in secure groups a group security policy defined as a statement of the entirety of security relevant parameters and facilities used to implement the group. This best fits the viewpoint of policy as defining how security directs group behaviour, who are the entities allowed to participate, and which mechanisms will be used to achieve mission critical goals.

The remainder of this paper is organized as follows. Section II explains the proposed system of this paper. Section III discusses the results of proposed system. Section IV draws some conclusion. Finally, Section V discusses the future work.

II. PROPOSED SYSTEM

1.User Interface Design

The goal of user interface design is to make the user's interaction as simple and efficient as possible, in terms of accomplishing user goals—what is often called user-centered design. Good user interface design facilitates finishing the task at hand without drawing unnecessary attention to it. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements (e.g., mental model) to create a system that is not only operational but also usable and adaptable to changing user needs.

2.Cloud Provider

A service provider offers customers storage or software services available through cloud. Usually, it means the storage and software is available for access via the Internet. Services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. Data owners, data consumers, domain authorities, and the trusted authority are organized in a hierarchical manner.

3. Domain Authorities

A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. In addition, we assume that communication channels between all parties are secured using standard security protocols, such as SSL. The trusted authority acts as the root of trust and authorize the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain.

4. Trusted Authority

The trusted authority is the root authority and responsible for managing top-level domain authorities. Each top-level domain authority corresponds to a top-level organization, such as a federated enterprise, while each lower-level domain authority corresponds to a lower-level organization, such as an affiliated company in a federated enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority is responsible for managing the domain authorities at the next level or the data owners/consumers in its domain.

5. Data Control System

In ASBE scheme, a data encryptor specifies an access structure for a cipher text which is referred to as the cipher text policy. Only users with decryption keys whose associated attributes, specified in their key structures, satisfy the access structure can decrypt the cipher text.

Key Structure: We use a recursive set based key structure as in where each element of the set is either a set or an element corresponding to an attribute.

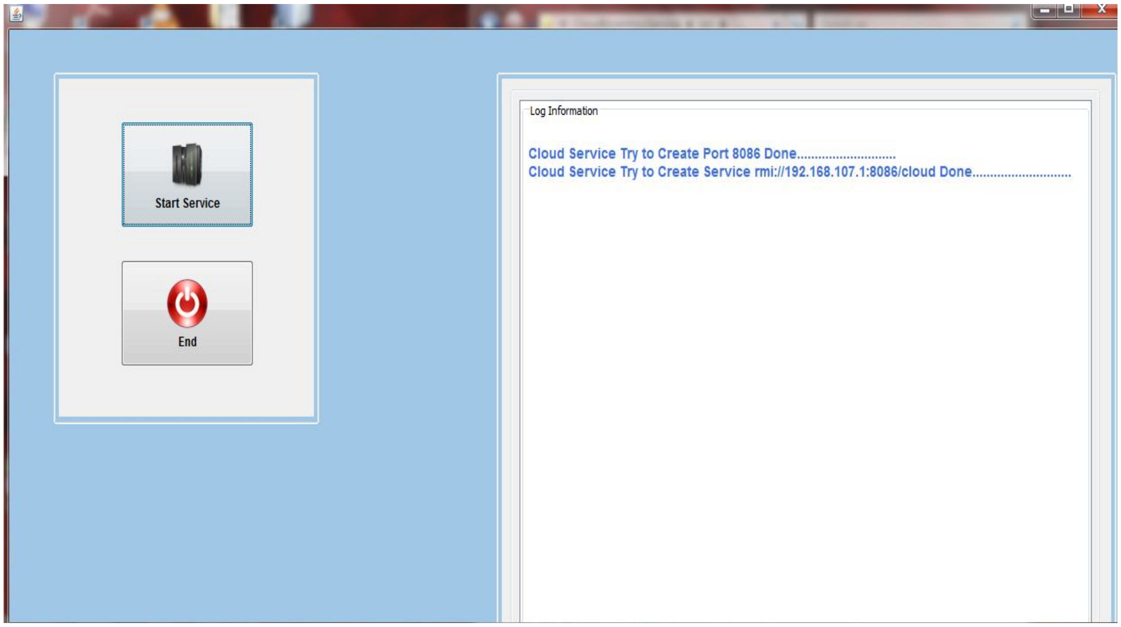
New File Creation: To protect data stored on the cloud, a data owner first encrypts data files and then stores the encrypted data files on the cloud. Before uploading to the cloud, a data file is processed by the data owner as follows:

- Pick a unique ID for this data file.
- Randomly choose a symmetric data encryption key, where is the key space, and encrypt the data file .

User Revocation: Whenever there is a user to be revoked, the system must make sure the revoked user cannot access the associated data files any more. One way to solve this problem is to re-encrypt all the associated data files used to be accessed by the revoked user, but we must also ensure that the other users who still have access privileges to these data files can access them correctly. ASBE inherits the advantage of efficient user revocation. We add an attribute to a user's key, which indicates the time until which the key is considered to be valid. Then the policy associated with data files can include a check on the attribute as a numerical comparison.

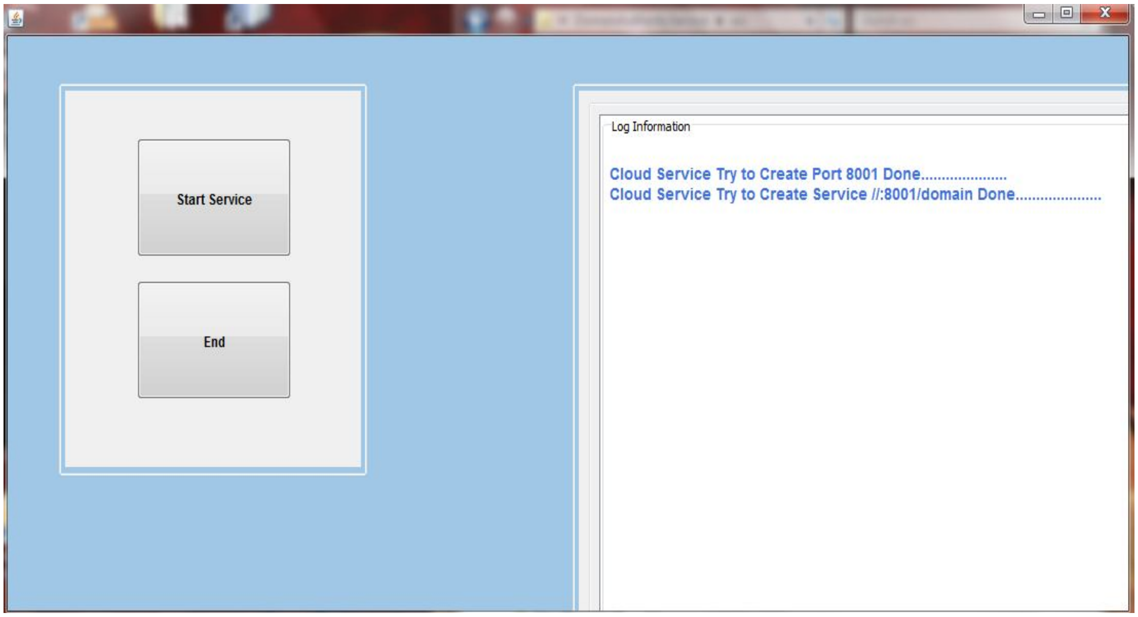
File Access: When a user sends request for data files stored on the cloud, the cloud sends the corresponding cipher texts to the user. The user decrypts them by first calling to obtain and then decrypt data files.

III. RESULTS



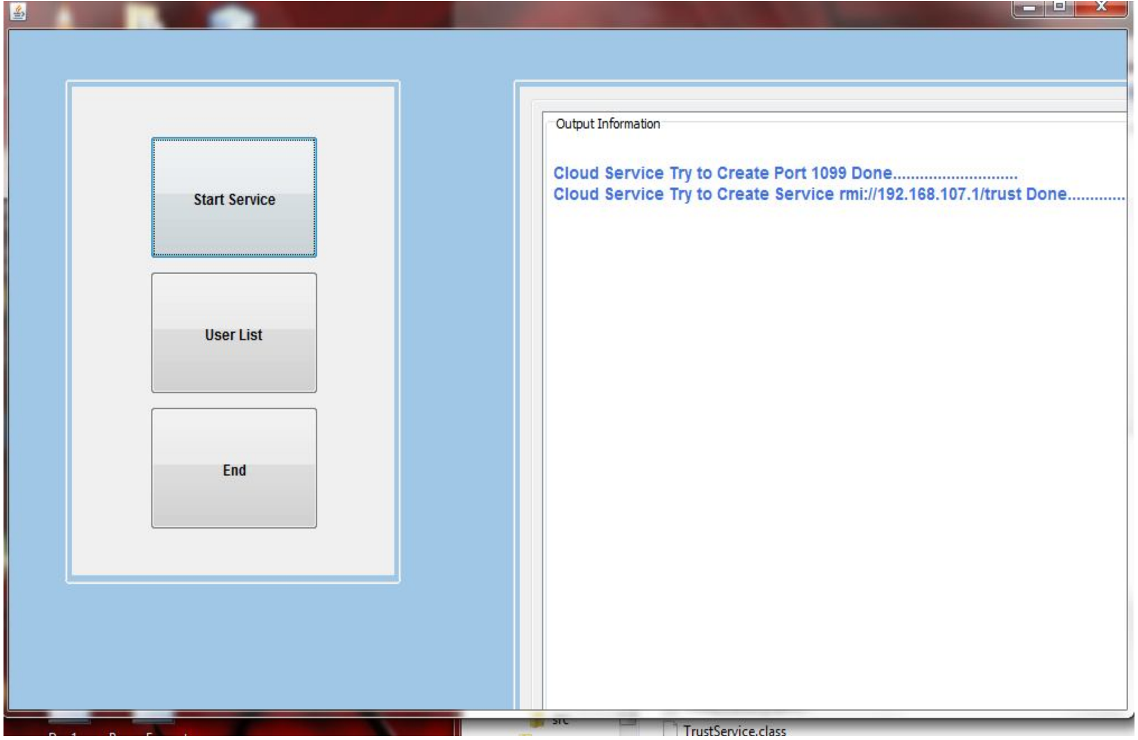
```
Cloud Service Try to Create Port 8086 Done...........................
Cloud Service Try to Create Service rmi://192.168.107.1:8086/cloud Done...........................
```

Figure 1.Cloud Inventory Service



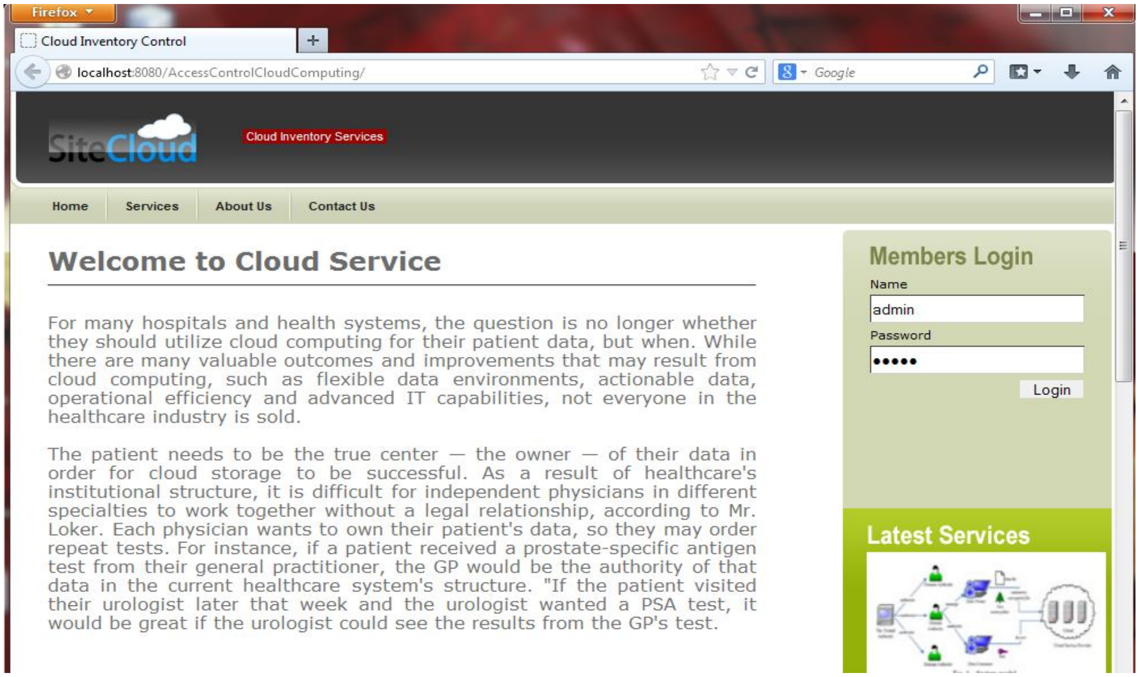
```
Cloud Service Try to Create Port 8001 Done.....................
Cloud Service Try to Create Service //:8001/domain Done.....................
```

Figure 2.domain authority



```
Cloud Service Try to Create Port 1099 Done............................
Cloud Service Try to Create Service rmi://192.168.107.1/trust Done............
```

Figure 3.Trusted authority



Welcome to Cloud Service

For many hospitals and health systems, the question is no longer whether they should utilize cloud computing for their patient data, but when. While there are many valuable outcomes and improvements that may result from cloud computing, such as flexible data environments, actionable data, operational efficiency and advanced IT capabilities, not everyone in the healthcare industry is sold.

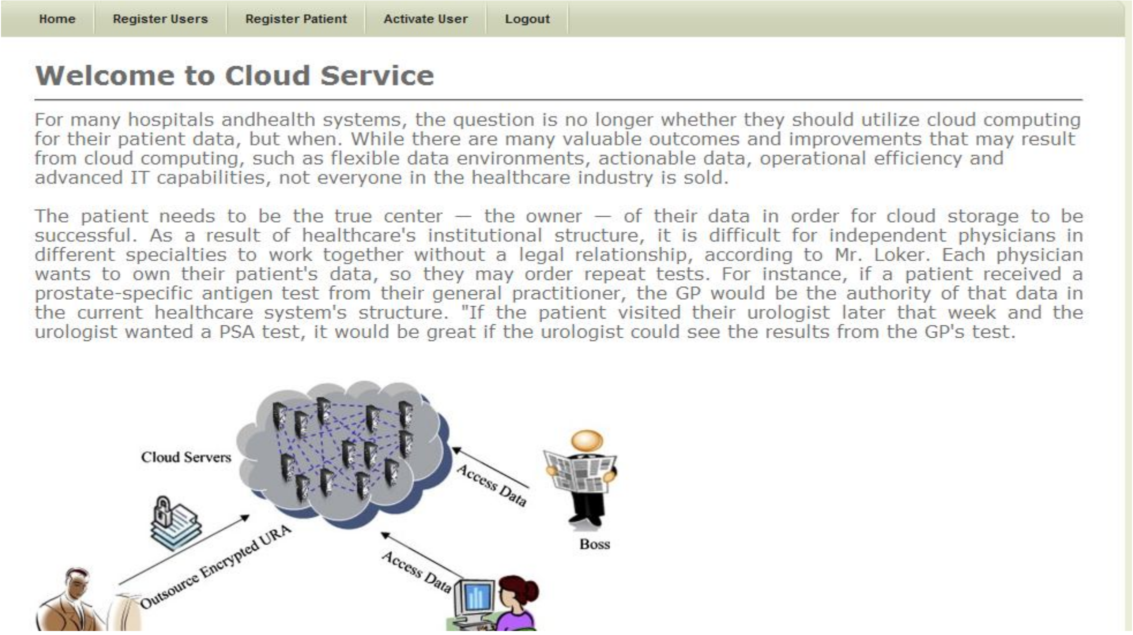
The patient needs to be the true center — the owner — of their data in order for cloud storage to be successful. As a result of healthcare's institutional structure, it is difficult for independent physicians in different specialties to work together without a legal relationship, according to Mr. Loker. Each physician wants to own their patient's data, so they may order repeat tests. For instance, if a patient received a prostate-specific antigen test from their general practitioner, the GP would be the authority of that data in the current healthcare system's structure. "If the patient visited their urologist later that week and the urologist wanted a PSA test, it would be great if the urologist could see the results from the GP's test.

Members Login

Name: admin

Password: •••••

Figure 4.login form

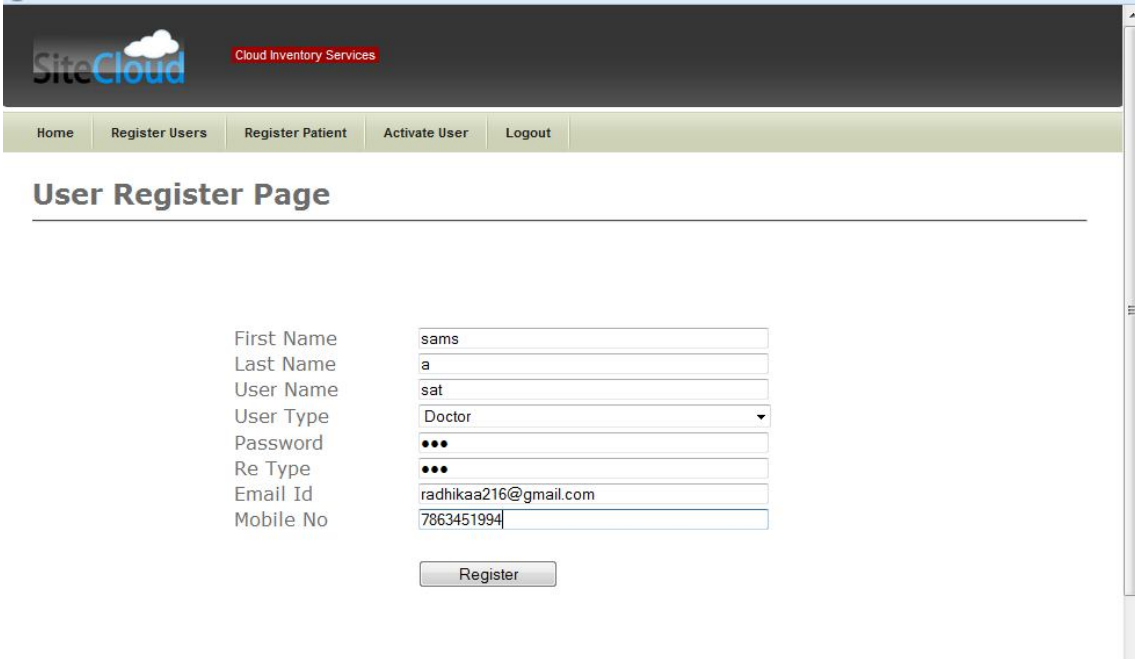


Welcome to Cloud Service

For many hospitals andhealth systems, the question is no longer whether they should utilize cloud computing for their patient data, but when. While there are many valuable outcomes and improvements that may result from cloud computing, such as flexible data environments, actionable data, operational efficiency and advanced IT capabilities, not everyone in the healthcare industry is sold.

The patient needs to be the true center — the owner — of their data in order for cloud storage to be successful. As a result of healthcare's institutional structure, it is difficult for independent physicians in different specialties to work together without a legal relationship, according to Mr. Loker. Each physician wants to own their patient's data, so they may order repeat tests. For instance, if a patient received a prostate-specific antigen test from their general practitioner, the GP would be the authority of that data in the current healthcare system's structure. "If the patient visited their urologist later that week and the urologist wanted a PSA test, it would be great if the urologist could see the results from the GP's test.

Figure 5. Trusted authority



User Register Page

First Name	sams
Last Name	a
User Name	sat
User Type	Doctor
Password	●●●
Re Type	●●●
Email Id	radhikaa216@gmail.com
Mobile No	7863451994

Figure 6. User register page

IV. CONCLUSION

In this paper, the issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, has been analyzed. The proposed framework of secure sharing of personal health records in cloud computing, considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. We utilize ABE to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliations.

V. FUTURE ENHANCEMENT

In future enhancement, Once a user needs to be revoked, the entire RL has to be sent, which raises a large amount of communication overhead. Also, in particular, the time for signature verification grows longer. To mitigate the communication overhead, we suggest to broadcast the RL that includes only additional revoked users. To restrain the signature verification delay, we propose a optimized threshold time to shorten RL. Moreover, the PR, TR, or RLS scheme is only appropriate respectively for single revocation situation, but in real applications the comprehensive scheme is required, which needs to synthesize three basic schemes co-ordinately.

REFERENCES

[1] Kui Ren, Ming Li, Shucheng Yu, Wenjing Lou, Yao Zheng, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption" IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 1, January 2013.

[2] Cong Wang, Kui Ren, Shucheng Yu and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", INFOCOM, 2010 Proceedings IEEE,march 2010.

[3] Cong Wang, Kui Ren, Shucheng Yu "Attribute Based Data Sharing with Attribute Revocation", ASIACCS '10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security 2010.

[4] Amit Sahaiz, Brent Waters, Omkant Pandeyy, Vipul Goyal"Attribute-Based Encryption for Fine-Grained Access Control", CCS '06 Proceedings of the 13th ACM conference on Computer and communications security 2006 .

[5] Ming Li, Ning Cao, Shucheng Yuy and Wenjing Lou "Authorized private keyword search over encrypted personal health records in cloud computing",Distributed Computing Systems (ICDCS), 2011 31st International Conference, June 2011

[6] Josh Benaloh, Kristin Lauter, ric Horvitz, Melissa Chase "Patient controlled encryption: ensuring privacy of electronic medical records", CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security.

[7] Ting-Yu,Winnslett.M, "A Unified Scheme for resource protection in automated trust negotiation", Security and Privacy 2003 Proceedings, May 2003.

[8] Amit Sahai, Brent Waters, Carnegie Mellon, John Bethencourt "ciphertext-policy attribute-based encryption",Security and Privacy, May 2007

[9] Kristin Lauter "Automated trust negotiation using cryptographic credentialsutility cloud computing and emerging it platforms:vision, hype, and reality for delivering computing",Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference Dec 2010.

[10]Brunelli.D "Cloud computing and emerging it platforms:vision, hype, and reality for delivering computing as the 5th utility ", Volume 25, Issue 6, June 2009

[11] Amit Sahai, Brent Waters, "fuzzy identity-based encryption",CCS '08 Proceedings of the 15th ACM conference on Computer and communications security 2008

[12] Mrinmoy Barua, Xiaohui Liang,"Principles of policy in secure groups PEACE: An Efficient and Secure Patient-centric Access Control Scheme for eHealth Care System",Computer Communications Workshops,IEEE Conference April 2011