ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (201-208), Month: October - December 2014, Available at: www.researchpublish.com

Sharing of PHR's in Cloud Computing

Dussa Manasa[1], K. Rajesh Khanna[2]

[1]M.Tech in Cse Dept, Vaagdevi Engineering College, Warangal, Andhra Pradesh, India
[2]Associate Professor in Cse Dept, Vaagdevi Engineering College, Warangal, Andhra Pradesh, India

Abstract: **Personal health records (PHRs) grant patients access to a wide range of health information sources, best medical practices and health knowledge. In patient centric secure sharing, patients will create, manage and control their personal health data from one place using the web. Prior to storing the records in cloud server, they are encrypted using encryption algorithm which ensures the patient's full control over their PHR. Patients only decide which set of users can access which set of files. In Attribute-Based Encryption the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.**

Keywords: **Attribute-based access control, Auxiliary attribute authorities, Electronic health records, Role-based access control, Security domains.**

I. INTRODUCTION

The term "personal health record" is not new. The earliest mention of the term was in an article indexed by PubMed dated June 1978, [2] and even earlier in 1956 reference is made to a personal health log. [3] However, most scientific articles written about PHRs have been published since 2000.

The term "PHR" has been applied to both paper-based and computerized systems; current usage usually implies an electronic application used to collect and store health data. In recent years, several formal definitions of the term have been proposed by various organizations. [4][5][6]

It is important to note that PHRs are not the same as electronic health records (EHRs). The latter are software systems designed for use by health care providers. Like the data recorded in paper-based medical records, the data in EHRs are legally mandated notes on the care provided by clinicians to patients. There is no legal mandate that compels a consumer or patient to store her personal health information in a PHR.

PHRs can contain a diverse range of data, including but not limited to: allergies and adverse drug reactions, chronic diseases, family history, illnesses and hospitalizations, imaging reports (e.g. X-ray), laboratory test results, medications and dosing, prescription record, surgeries and other procedures, vaccinations and Observations of Daily Living (ODLs).

There are two methods by which data can arrive in a PHR. [1] A patient may enter it directly, either by typing into fields or uploading/transmitting data from a file or another website. The second is when the PHR is tethered to an electronic health record, which automatically updates the PHR. Not all PHRs have the same capabilities, and individual PHRs may support one or all of these methods. [1]

In addition to storing an individual's personal health information, some PHRs provide added-value services such as drug-drug interaction checking, electronic messaging between patients and providers, managing appointments, and reminders.[7]

In this paper, we propose a novel and practical framework for fine-grained data access control to PHR data in cloud computing environments, under multiowner settings. To ensure that each owner has full control over her PHR data, we

leverage attribute-based encryption (ABE) as the encryption primitive, and each owner generates her own set of ABE keys. In this way, a patient can selectively share her PHR among a set of users by encrypting the file according to a set of attributes, and her encryption and user management complexity is linear to the number of attributes rather than the number of authorized users in the system.

To avoid from high key management complexity for each owner and user, we divide the system into multiple security domains (SDs), where each of them is associated with a subset of all the users. Each owner and the users having personal connections to her belong to a personal domain, while for each public domain we rely on multiple auxiliary attribute authorities (AA) to manage its users and attributes. Each AA distributive governs a disjoint subset of attributes, while none of them alone is able to control the security of the whole system. In addition, we discuss methods for enabling efficient and on-demand revocation of users or attributes, and break-glass access under emergence scenarios.

1.1. Our Contributions

Traditionally, research on access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. Various access control models have been proposed and applied, including role-based (RBAC) and attribute-based access control (ABAC) [10]. In RBAC [11], each user's access right is determined based on his/her roles and the role-specific privileges associated with them.

Symmetric key cryptography (SKC) based solutions. Vimercatiet.al. proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods [13], which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable. In [4], files in a PHR are organized by hierarchical categories in order to make key distribution more efficient. However, user revocation is not supported. In [6], an owner's data is encrypted block-by-block, and a binary key tree is constructed over the block keys to reduce the number of keys given to each user.

II. RELATED WORK

Traditionally, research on access control in electronic health records (EHRs) often places full trust on the health care providers where the EHR data are often resided in, and the access policies are implemented and enforced by the health providers. Various access control models have been proposed and applied, including role-based (RBAC) and attribute-based access control (ABAC) [10]. In RBAC [11], each user's access right is determined based on his/her roles and the role-specific privileges associated with them. The ABAC extends the role concept in RBAC to attributes, such as properties of the resource, entities, and the environment. Compared with RBAC, the ABAC is more favourable in the context of health care due to its potential flexibility in policy descriptions [10]. A line of research aims at improving the expressiveness and flexibility of the access control policies [12].

Attribute-based encryption (ABE). The SKC and traditional PKC based solutions all suffer from low scalability in a large PHR system, since file encryption is done in an one-to-one manner, while each PHR may have an unpredictable large number of users. To avoid such inconveniences, novel one-to-many encryption methods such as attribute-based encryption can be used [15]. In the seminal paper on ABE [16], data is encrypted to a group of uses characterized by a set of attributes, which potentially makes the key management more efficient. Since then, several works used ABE to realize fine-grained access control for outsourced data [17,18,19,20]. However, they have not addressed the multiple data owner settings, and there lacks a framework for patient-centric access control in multi-owner PHR systems. Note that, in [21] a single authority for all users and patients is adopted. However, this suffers from the key escrow problem, and patients' privacy still cannot be guaranteed since the authority has keys for all owners. Recently Ibraimi et.al. [22] applied ciphertext policy ABE (CP-ABE) [23] to manage the sharing of PHRs. However, they still assume a single public authority, while the challenging key-management issues remain largely unsolved.

III. PROPOSED WORK

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

3.1. Modules

1. Registration
2. Upload files
3. ABE for Fine-grained Data Access Control
4. Setup and Key Distribution
5. Break-glass

3.1.1. Modules Description

3.1.1.1. Registration

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data readers have access to.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - *public domains*
- PSD - *personal domains*
- AA - attribute authority
- MA-*ABE* - multi-authority ABE
- KP-ABE - key policy ABE

3.1.1.2. Upload files

In this module, users upload their files with secure key probabilities. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

3.1.1.3. ABE for Fine-grained Data Access Control

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

3.1.1.4. Setup and Key Distribution

In this module the system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access.

Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN)

There are two ways for distributing secret keys.

- First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in GoogleDoc.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (201-208), Month: October - December 2014, Available at: www.researchpublish.com

 Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate the user secret key that embeds her access structure.

3.1.1.5. Break-glass module

In this module when an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In our framework, each owner's PHR's access right is also delegated to an emergency department ED to prevent from abuse of break-glass option, the emergency staff needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

IV. PROBLEM STATEMENT AND ASSUMPTIONS

4.1. Problem Definition

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data.

V. IMPLEMENTATION

The implementation environment has software such as ASP.NET in Windows XP operating system. The system uses ASP.NET with C# and SQL server 2005

The Login Screen provides the login for the new user and the already existing user. Existing user can login directly by entering the username and the password. If he is a new user then he has to register.

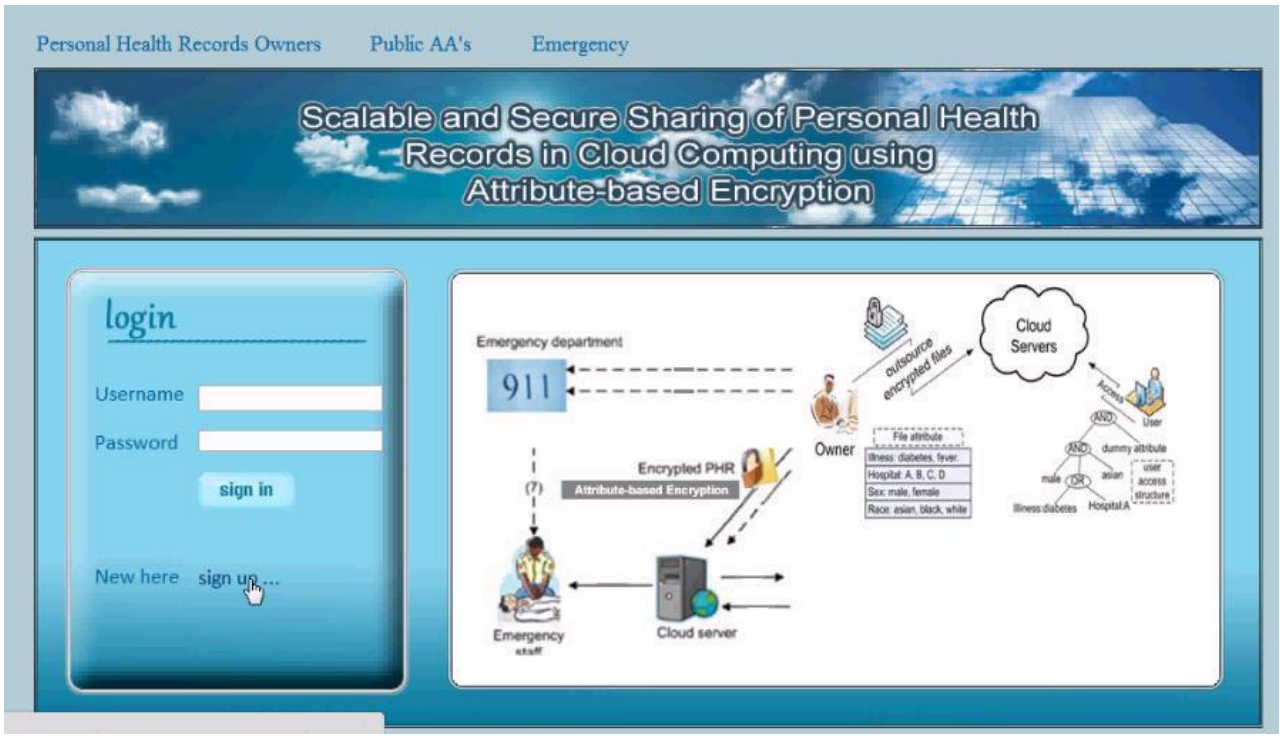

Fig.1 screen shot for user login

For the registration the user has to enter the id, name, username, password, mobile name, email id and date of birth.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (201-208), Month: October - December 2014, Available at: www.researchpublish.com

Fig .2 Register Page

After the successful registration the user gets the symmetric key and the public key.

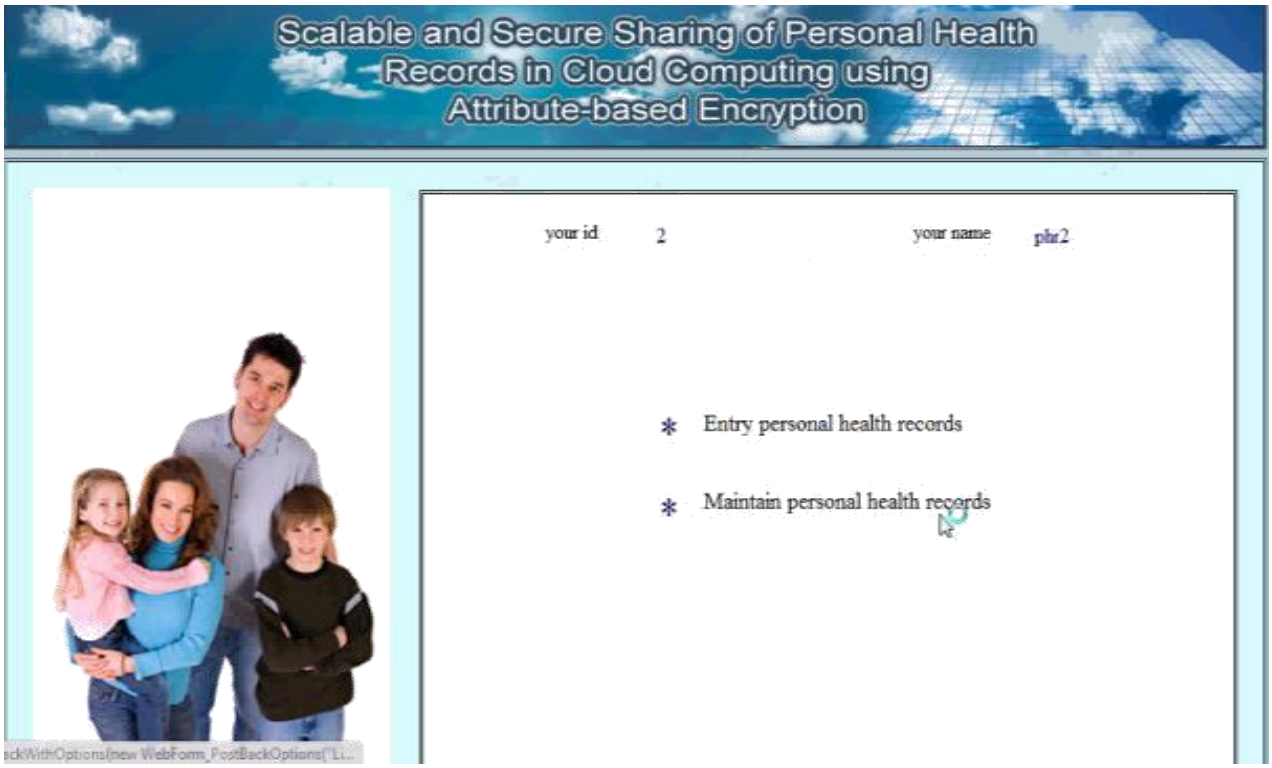

Fig.3 admin successful login

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (201-208), Month: October - December 2014, Available at: www.researchpublish.com

Admin has the following options enter personal health records and maintain personal health records.

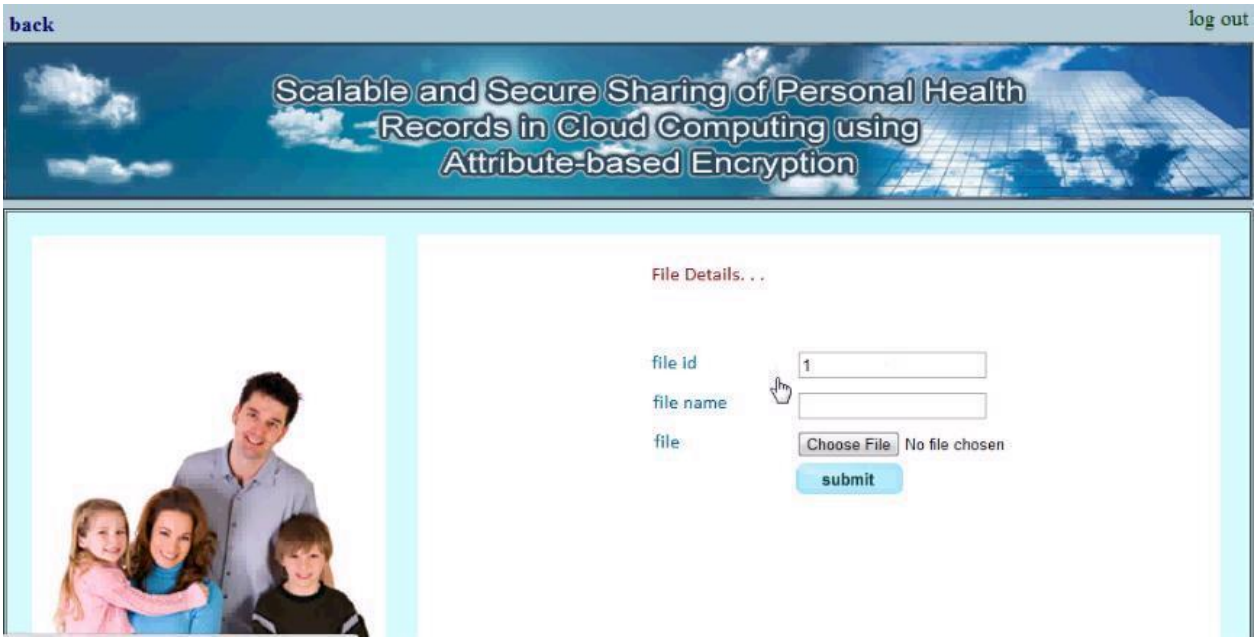

Fig.4 File Upload

Files can be uploaded by file id, file name and select the file to upload. Clicks submit to upload a file.

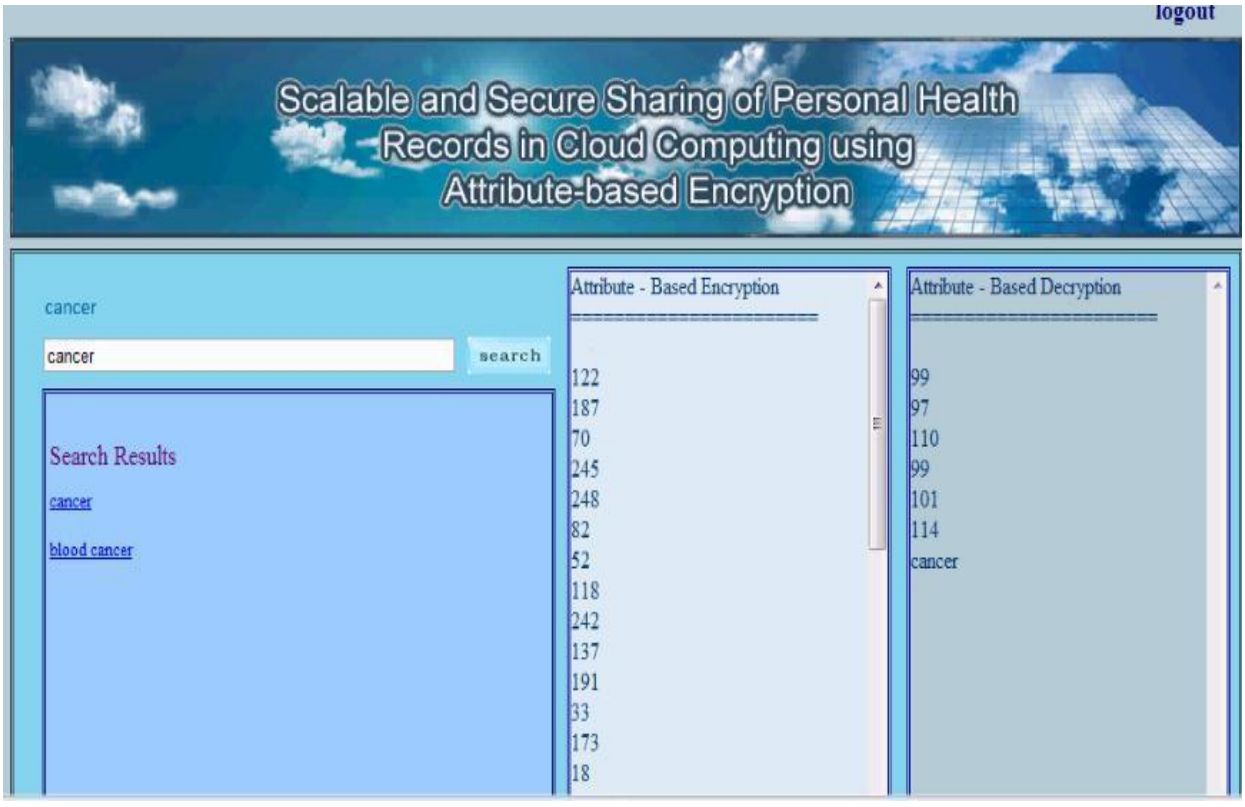

Fig.5 Search file by user

Enter the keyword for the disease and click search to search the records corresponding to the disease. To download the file the user need to enter the symmetric key. If the symmetric key entered is wrong then the user is blocked.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (201-208), Month: October - December 2014, Available at: www.researchpublish.com

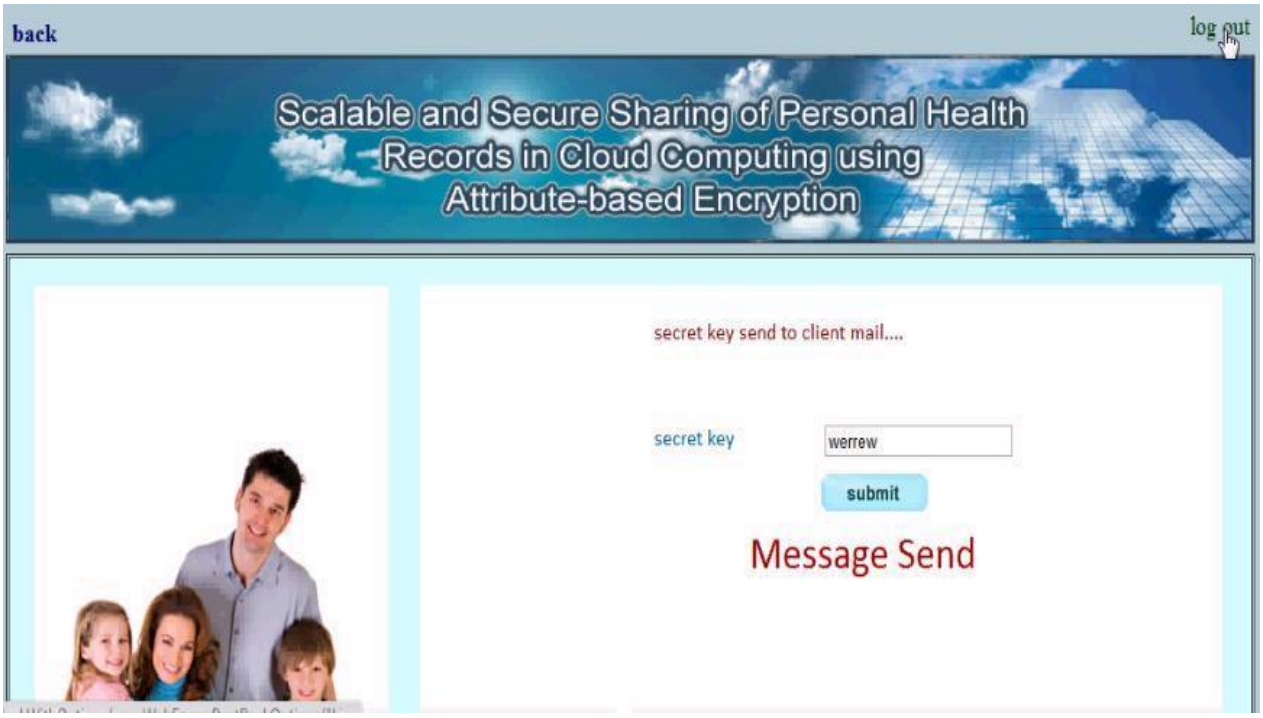

Fig.6 Secret Key to the Mail

When the user needs the secret key he has to send a request by verifying the email. After the secret key generation it is send directly to the mail.

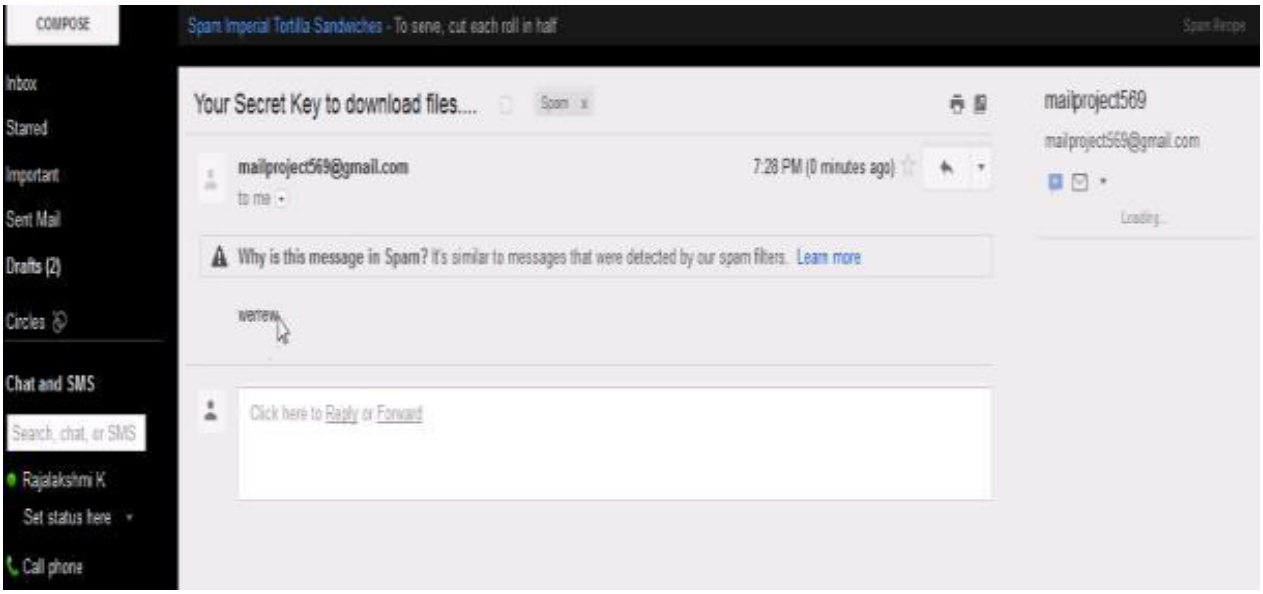

Fig.7 Secret Key to Mail

VI. CONCLUSION

In this paper, we have proposed a novel framework of access control to realize patient-centric privacy for personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that patients shall have full 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 when the number of owners and users in the system is large. We utilize multi-authority attribute-based encryption to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from different public

domains with different professional roles, qualifications and affiliations. An important future work will be enhancing the MA-ABE scheme to support more expressive owner-defined access policies.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.

[2] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act," http://www.cms.hhs.gov/HIPAAGenInfo01_ Overview.asp , 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/ 48/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/ health he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records.

[8] Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

Dussa Manasa received the B.Tech Degree in Computer Science & Engineering from Balajii Institute of Technology and Science, Warangal, A.P, India. Currently doing M.tech in Computer Science & Engineering at Vaagdevi Engineering College, Warangal, India. Research interests include ,Network security, Computer Network etc.,

Kaluva Rajesh Khanna received the M.Tech Degree in Computer Science and Engineering from JNTU, Hyderabad, Currently he is working as an Assistant Professor at Vaagdevi Engineering college, Warangal.His research areas include -network security etc.,