IMPROVING DATA SECURITY USING ATTRIBUTE BASED BROADCAST ENCRYPTION IN CLOUD COMPUTING

[1]K.Kamalakannan, [2]Mrs.Hemlathadhevi

Abstract -- Personal health record (PHR) is an patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing using attribute-based encryption (ABE) techniques. The users in the PHR system is divided into two domains Personal domain(PSD) and Public domain(PUD).The Personal domain(PSD) consists of users such as family members and friends related to the patient(data owner).The Public domain(PUD) consists of users based on their roles such as doctors, pharmacists and nurses. Creating a Cloud space to store all the patient information about his personal dosage and his medical history. Changing the authentication with respect to the Role of the Logged in users such as Doctors, Nurses and Pharmacist to give options to user based on the logged in user. The patient information stored in Cloud is encrypted using the Attribute based encryption.In the Proposed system the data is encrypted using Attribute based broadcast encryption(ABBE).The data will be broadcast to the set of authorized users.It will improve security to the data that is stored in the cloud.

Keywords: Personal health records, Attribute-based encryption, Data privacy, Attribute-based broadcast encryption.

I. INTRODUCTION

In order to protect the personal health data stored on a semi trusted server, the attribute based encryption (ABE) is used as the main encryption primitive.

- ***Kamalakannan.K*** *is currently pursuing master degree program in computer science engineering. Ph-9840310803.*
- ***Hemalathadhevi.A****, M.E., A.P/ CSE Dept, Ph-9790872181*

The main aim of the project is to improve security to the personal health data that are stored in the cloud using Attribute based broadcast encryption techniques(ABBE). Cloud computing is an expression used to describe a variety of computing concepts that involve a large number of computers connected through a real-time communication network such as the Internet. Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally. Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to re-evaluate decisions about existing resources.

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Chapter 2 discusses about the literature survey emphasizing the research activities and related works in cloud computing and overview the drawbacks of existing system and about the proposed system. Chapter 3 presents the secure sharing of personal health data architecture. Chapter 4 explains the implementation of different modules. Chapter 5 mentions the concluding remarks about the project.

II. RELATED WORKS

Attribute Based Broadcast Encryption (ABBE) is a novel Broadcast Encryption (BE) approach. Compared to existing BE [2] approaches that requires an explicitly specified decrypters list, ABBE encrypter enforces an expressive access policy composed of one or more attributes. Although ABBE is more flexible and efficient with reduced storage overhead, cipher text size of current ABBE schemes [1] is linearly proportional to the numbers of attributes. In this paper, we investigate the solution on how to reduce the ABBE's cipher text size to a constant value. Moreover, we explore the capability of using ABBE in secure many-to-many communication environments.

A broadcast encryption system allows a broadcaster to send an encrypted message to a dynamically chosen subset *RS*, |*RS*| = *n*, of a given set of users, such that only users in this subset can decrypt the message. An important component of broadcast encryption schemes is revocation of users by the broadcaster, thereby updating the subset *RS*. Revocation may be either temporary, for a specific ciphertext, or permanent. We present the first public key broadcast encryption scheme with permanent revocation of users, unlike all previous public key schemes that support temporary revocation. The system explores the challenge of preserving patients' privacy in electronic health record systems. We argue that security in such systems should be enforced via encryption as well as access control. Furthermore, we argue for approaches that enable patients to generate and store encryption keys, so that the patients' privacy is protected should the host data center be compromised. The standard argument against such an approach is that encryption would interfere with the functionality of the system.

Secure management of Electronic Health Records (EHR) in a distributed computing environment such as cloud computing where computing resources including storage is provided by a third party service provider is a challenging task. In this paper, we explore techniques which guarantees security and privacy of medical data stored in the cloud. We show how new primitives in attribute-based cryptography can be used to construct a secure and privacy-preserving EHR system that enables patients to share their data among healthcare providers in a flexible, dynamic and scalable manner. Attribute-based cryptographic primitives provides flexible policies which can be used to build secure infrastructure for designing privacy preserving electronic health record system.

III. PROPOSED SYSTEM

The Attribute based broadcast encryption techniques(ABBE) is used to improve security for the personal health data(image) stored in the cloud. The Attribute based broadcast encryption techniques(ABBE) allows the broadcaster to send an encrypted data to the set of users such as family doctor, specialized doctor and family members or friends. The authorized users only decrypt the personal health data(image) who are provided with the decrypt key. A Attribute based broadcast encryption techniques*(ABBE)* provides flexibility of expressive access Policy in many to many communications.

The system mainly enables the Permanent Revocation and the collusion-resistant during access mechanism. ABBE encryption enforces an expressive access policy composed of attributes that specify the entities who can decrypt the data. The model of ABBE is conceptually close to role based access control used to describe the role of the users and to provide the efficient and flexible data access policy. The system architecture for sharing the personal health record or data to users and data access in cloud is shown in the below Fig 1.

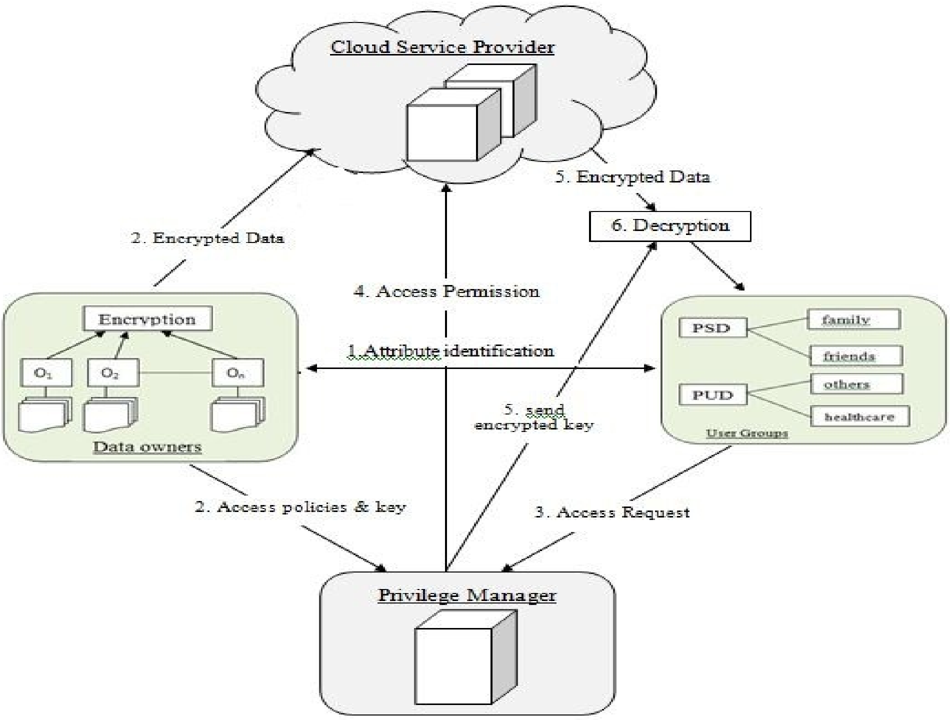


Fig 1 Attribute-Based Encryption Scheme

3.1 Key Generation and Authorisation

The keys are generated to the users at the time of their registeration by the admin. The Key Generation and Authorisation module is designed to verify the users with their roles. Authority permissions are initiated by the admin. The user will be given a username, password, public key for access into the system. The user entering the wrong username, password or public key will not given permission to access into the system. The private key generated for the user will be used to decrypt the personal health data.

3.2 Encryption using Attribute-Based Encryption

The data is encrypted using ABE and will be stored in the cloud. The attribute used in this is the Private key of the data owner. The private key is used to encrypt the PHR and will be stored in the cloud. A data Owner can update the sharing policy for an existing data by updating the attributes. The supported operations include add, delete, modify which can be also done by the user. The Private key generated by the user will be used to decrypt the PHR based on their roles.

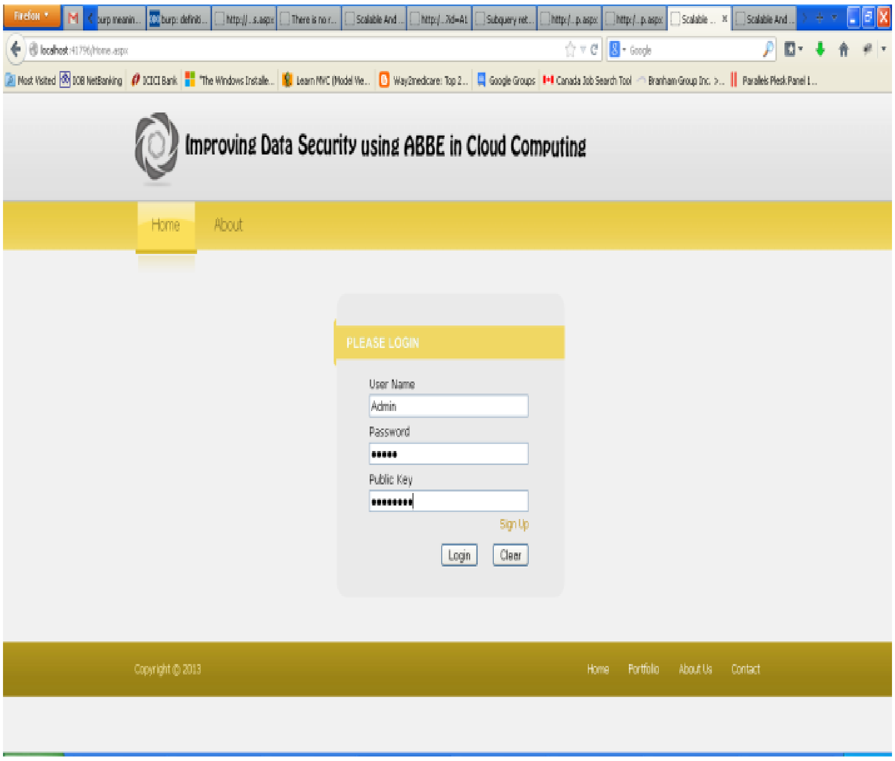
3.3 Encryption using Attribute-Based Broadcast Encryption

The Attribute based broadcast encryption techniques(ABBE) allows the broadcaster to send an encrypted data to the set of users. The Attribute based broadcast encryption techniques(ABBE) will provide efficient and flexible data access policy. It will also enhance the security provided by the existing system. It mainly enables the Permanent Revocation and the collusion-resistant during access mechanism.

3.4 Revocation

The act of recalling or terminating a previously granted power of attorney. Broadcast encryption supports temporary revocation of users if revoked users are excluded from the set. Broadcast encryption also supports permanent revocation of users if revoked users cannot decrypt any cipher text after revocation.

IV EXPERIMENTAL RESULTS & SCREENSHOTS



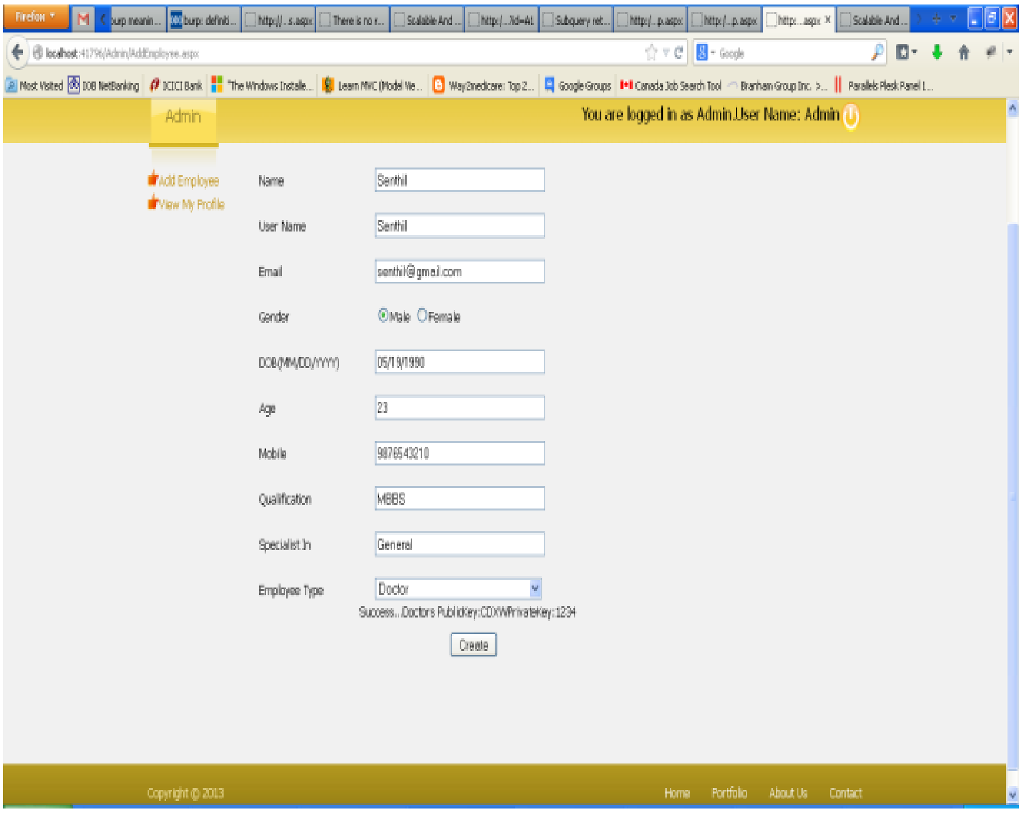
Improving Data Security using ABBE in Cloud Computing

PLEASE LOGIN

User Name: Admin

Password: •••••

Public Key: ••••••••



You are logged in as Admin.User Name: Admin

Name: Senthil

User Name: Senthil

Email: senthil@gmail.com

Gender: ● Male ○ Female

DOB(MM/DD/YYYY): 05/19/1990

Age: 23

Mobile: 9876543210

Qualification: MBBS

Specialist In: General

Employee Type: Doctor

Success...Doctors PublicKey:CDXWPrivateKey:1234

V CONCLUSIONS AND FUTURE ENHANCEMENT

The PHR owner encrypts the data that will be stored in the cloud. The users in the PHR system is divided into two domains Personal domain(PSD) and Public domain(PUD).The Personal domain(PSD) consists of users such as family members and friends related to the patient(data owner).The Public domain(PUD) consists of users based on their roles such as doctors, pharmacists and nurses. The users will access the personal health data by entering their keys provided by the admin at the time of their registeration. The list of users in the public domain is unpredictable so there may be some privacy concerns to the data.

Second phase of the system is focused on enhancing the security. The reason for improving security is users in the public domain can access data for their usage. The Attribute based broadcast encryption techniques(ABBE) allows the broadcaster to send an encrypted data to the set of users such as family doctor, specialized doctor and family members or friends. The authorized users only decrypt the personal health data(image) who are provided with the decrypt key. So that Personal health data can be accessed only by the authorized set of users.

VI 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. Lo¨ hr, 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 AccountabilityAct,”http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp,2012.
[5] “Google, Microsoft Say Hipaa Stimulus Rule Doesn’t Apply to Them,” http://www.ihealthbeat.org/Articles/2009/4/8/,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.

[1]Kamalakannan.K received degree B.E Computer Science and Engineering from Alpha College of Engineering, Anna university in 2011. Now pursuing M.E Computer Science and Engineering in Meenakshi College of Engineering, Anna university, Chennai. Ph- 9840310803.

[2]Hemalathadhevi.A received the B.E(CSE) from Madras Institute of technology in 2004 and ME(CSE) from Anna University, Trichy in 2010. Currently, She is doing Ph.d in St.Peter’s University and working as Assistant Professor in the Computer Science Department, from Meenakshi College of Engineering. ph-9790872181.