Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 47 (2015) 22 – 29

Procedia Computer Science

Symptoms based treatment based on Personal Health Record using cloud computing

Dhivya .P, Roobini.S, Sindhuja.A,

1Assistant Professor, Department of Computer Science and Engineering
2,3Student, Department of Computer Science and Engineering SNS College of Technology, Coimbatore,India

Abstract

Cloud architecture is used for maintaining the personal health record and provide symptoms based treatment to the patients. The details of a patient need to be stored in a secured manner. It is to create a cloud storage server for long term storage over the internet. The storage server will act as a database server. Uploaded data stored in the cloud server through proxy re-encryption method. A secured threshold proxy re-encryption server and integrates it with a decentralized erasure code such that a secure distributed storage system. To generate proxy re-encryption key for one-time data access. A proxy server will be created virtually for one time data access. We can achieve the symptoms based treatment by secure Personal Health Record in cloud storage when applying the proposed encryption algorithm.

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)

Keywords:PersonalHealth Record(PHR),Encryption, proxy, treatments, cloud computing

1. Introduction

A personal health record is a collection of information about patient's health. They have probably encountered the big drawback of paper records. The hospital may rarely have their details with him. The Electronic personal health record systems remedy that problem by making patient's personal health record accessible to patients anytime via a web enabled device, such as Computer, Phone or Tablet. Personal health records are not the same as electronic medical records, which are owned and operated by doctor's offices, hospitals or Health insurance plans. There are growing number of doctor's offices using these systems, but those that do often limit the access to and control of the medical records.

Monitoring and updating on the patient's health conditions is done on a monthly basis.Based on monitored results, the doctors give their suggestions. This suggestion is purely hypothetical on the patient's

*Coresponding author Email: dhivyasnsce@gmail.com

Peer-review under responsibility of organizing committee of the Graph Algorithms, High Performance Implementations and Applications (ICGHIA2014)
doi:10.1016/j.procs.2015.03.179

condition and leads to a list of diseases that are prone to occur based on their symptoms, resulting in the patients having a prior knowledge of the body conditions and the diseases that are likely to occur. Thus, the patient's can be extra precautions about their health and can take the appropriate treatments. Personal Health Record (PHR) is an emerging patient-centric model of health information exchange. The personal health records are stored in the cloud servers. General encryption schemes protect data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data. Constructing a secured storage system that supports multiple functions is challenging when the storage system is distributed and has no central authority.

1.1 Cloud Computing

Cloud Computing is the delivery of computing services over the Internet. Cloud Services allow individuals and businesses to use software and hardware that are managed by third parties. Examples of cloud services include online file storage, social networking sites, web mail, and online business applications The cloud computing model allow access to information and computer resources from anywhere that a network connection is available. Definition of cloud computing has been developed by the U.S.National Institute of Standards and Technology(NIST).

Cloud computing is a model for enabling convenient,on-demand network access to a shared pool of configurable computing resources(e.g.,networks,servers,applications,and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics,three service models and four deployment models.

1.2. Cloud concept

Individual users connect to the cloud from their own personal computers or portable devices ,over the internet. To these individual users, the cloud is seen as a single application, device, or document. The hardware in the cloud(and the operating system that manages the hardware connections) is invisible. This cloud architecture is deceptively simple, although it does require some intelligent management to connect all those computers together and assign task processing to multitudes of users.

1.3. Types of clouds

There are different types of clouds that can subscribe depending on our needs.As a home user or small business owner, it will most likely use public cloud services.

- Public cloud – A public cloud can be accessed by any subscriber with an internet connection and access to the cloud space.
- Private cloud – A private cloud is established for a specific group or organization and limits access to just group.
- Community cloud – A community cloud is shared among two or more organizations that have similar cloud requirements.
- Hybrid cloud- A hybrid cloud is essentially a combination of atleast two clouds, where the clouds included are a mixture of public, private, or community.

2. **Existing System**

A novel patient-centric framework and a suite of mechanisms are proposed for data access control to PHRs stored in semi trusted servers. To achieve fine grained and scalable data access control for PHR's, attribute based encryption(ABE) techniques are leveraged to encrypt each patient's PHR file. Different from the single data owner scenario considered in most of the existing work, the focus is on the multiple data owner scenario, and the users in the PHR system are divided into multiple security domains that greatly reduce the key management complexity for owners and users. This method is more efficient and secure than a straightforward application of CP-ABE in which each organization acts as an authority that governs all types of attributes. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. The scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

2.1. Disadvantages Of Existing System

- General encryption schemes protact data confidentiality, but also limit the functionality of the storage system because a few operations are supported over encrypted data.
- Data robustness is a major requirement for storage systems.
- Constructing a secure storage system that supports multiple functions is challenging when the storage system is diatributed and has no central authority.

3. **Proposed System**

The main idea is to provide the treatment to the patient's based on the symptoms. Patient's information is stored in a third party's cloud system causes serious concern on data of the patient confidentiality. In order to provide strong confidentiality for message in storage servers, a user can encrypt message by a cryptographic method before applying an erasure code method to encode and store messages. When the user wants to use a message, the user needs to retrieve the codeword symbols from storage servers, decode them, and then decrypt them by using cryptographic keys.

3.1. Advantages

- It is focused on designing a cloud storage system for robustness, confidentiality, functionality.
- A cloud storage system is considered as a large scale distributed storage system that consists of many independent storage servers.
- Attribute based encryption was implemented for providing user rights to the viewers.
- Actors are implemented for role based data encryption and decryption.

4. **Use Case Diagram**

Fig

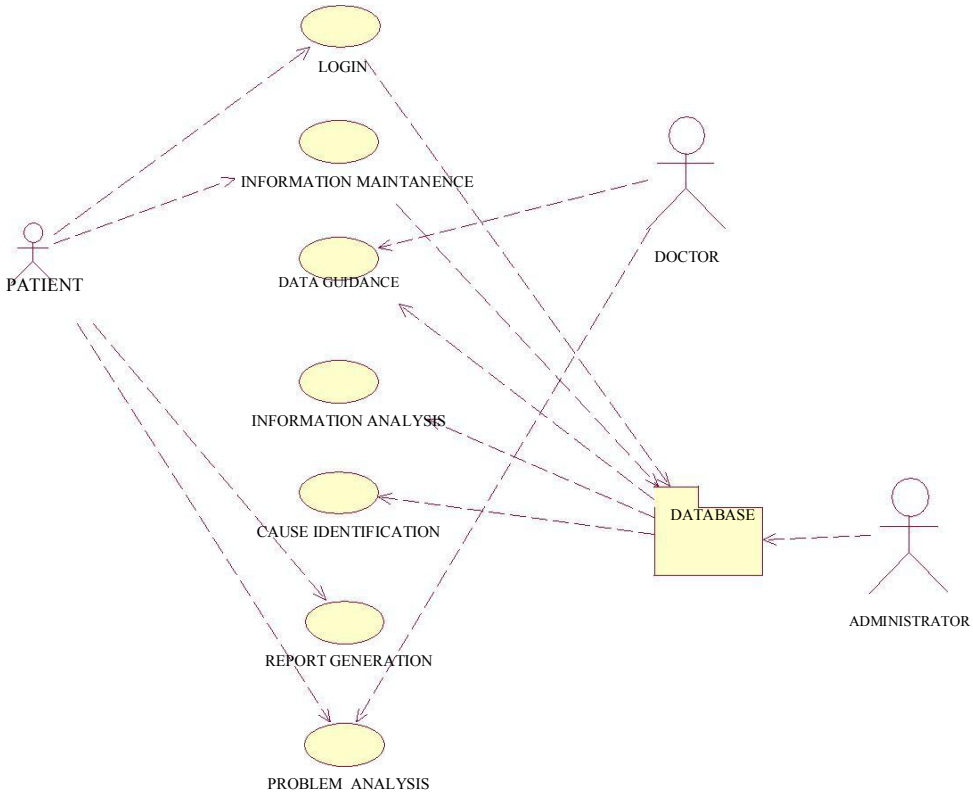

Fig 1. Use Case Diagram

5. **Methodology**

Using third party storage system tremendous number of data can be stored. It can be easily accessed using query distribution methods. The patient details will be clustered and can able to update in the third party storages through web.

Examples: The services provided to the patient are

- Primary care (Treatment history) doctors name and phone number.
- Finger print and iris details of the patient (Updatable).
- Allergies, including drug allergies.
- Chronic health problems such as high blood pressure.
- Major surgeries with dates.
- Living will or advance directives.

5.1. Construction Of Secure Cloud Storage

All the created information will be stored in the secured cloud architecture. The Patient information and treatment history is available in the encrypted format so the construction of the cloud will be more secured. The encryption will be done before the data reaches the server. This is to avoid hacking of data from internal hacker. The two biggest concerns about cloud storage are security and reliability. The storage server will be unique which has been distributed into much system for easy access of data. It contains only the encrypted data of the data owners. Third party accessing the data, they need prior authorization from the data owner. To implement this, a hybrid cryptographic method of key generation is introduced and this key is sent by the cloud server. The actors will interact with the proxy server using the authorized key. When the actor applies the key, they can view the requested data in the proxy server. The validation of key is the one time login only. In case viewing the data for next time means, they should get a new key from the data owner side. It works more efficient on cloud systems. Proxy re-encryption schemes are similar to traditional symmetric or asymmetric encryption schemes. It allows a message recipient to generate a re-encryption key based on his secret key and the key of the delegated user. This re-encryption key is used by the proxy as input to the re-encryption function, which is executed by the proxy to translate cipher texts to the delegated user's key. Asymmetric proxy re-encryption schemes come in bi-directional and unidirectional varieties. Proxy re-encryption schemes allow for a cipher text to be re-encrypted an unlimited number of times. Proxy re-encryption should not be re-encrypted an unlimited number of times.

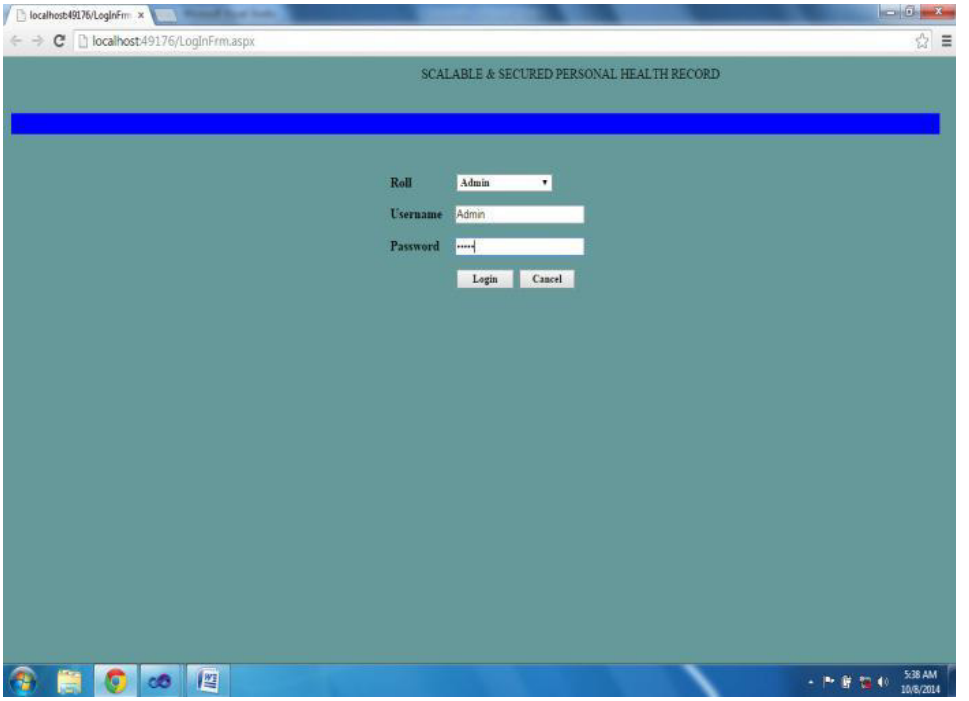

Fig 2.Login Page

52. ***Data Owner Authorization***

Here in case of a third party accessing the data command they need prior authorization from the data owner. In order to implement this, a hybrid cryptographic method of key generation is introduced. When doctor, insurance agent or another user trying to accssing the sensitive means, they should get an authorized key from the data owner. This key will be send by the cloud server. The problem of constructing an erasure code for storage over a network is considered when the data source are distributed in the cloud server. Specifically, it is assumed that there are n storage nodes with limited memory and k<n sources generating the data. A data collector is required, who can appear anywhere in the network for accessing the data, to query any k storage nodes and be able to retrieve the data. Decentralized Erasure Codes are introduces, which are linear codes with a specific randomized structure inspired by network coding on random bipartite graphs with encrypted format. It is shown that decentralized erasure codes are optimally sparse, and lead to reduce communication, storage and computation cost over random linear coding over the cloud server.

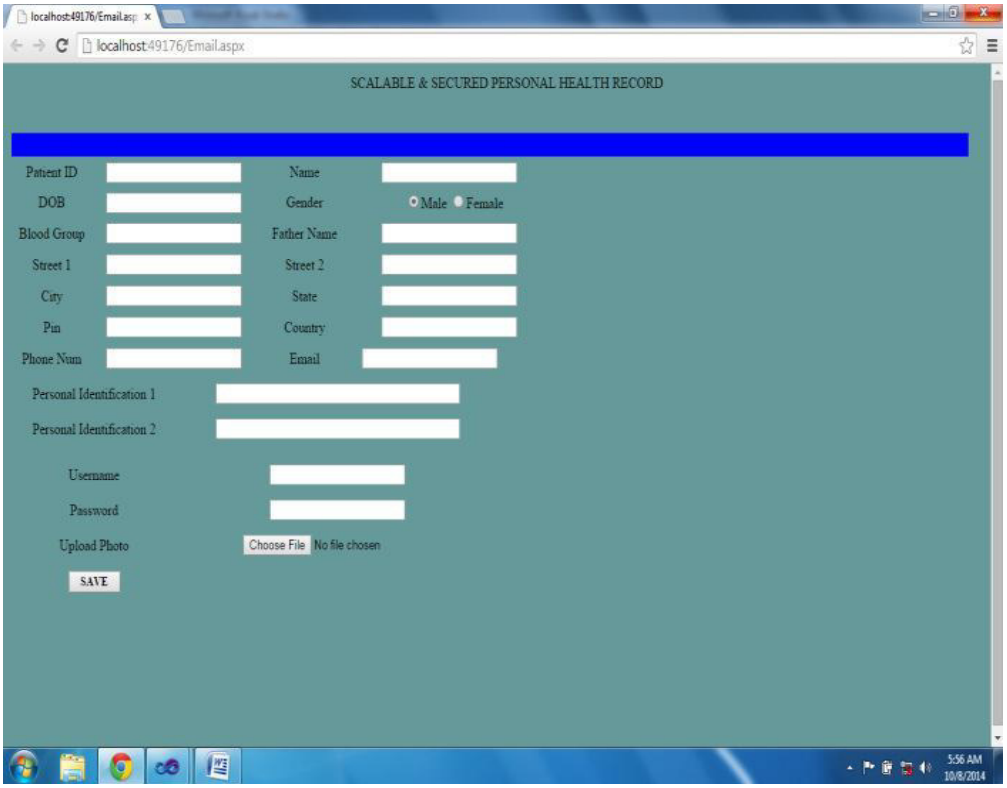

Fig 3. ***Create patient details***

5.3. proxy re-encryption

This is the final model of this project.Here the actors will interact with the proxy server using the authorized key. It is one of the advanced encryption model which works on both real system and virtual systems. When the actor applies the key, they can view the requested data in the proxy server. The validation of key is the one time login only. In case viewing the data for another time means, they should

get a new key from the data owner side. This works more efficient on cloud systems. Proxy re-encryption schemes are cryptosystems which allow third-parties (proxies) to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another. Proxy re-encryption schemes are similar to traditional symmetric or asymmetric encryption schemes. It allows a message receipient (key holder) to generate a re-encryption key based on his secret key and the key of the delegated user. This re-encryption key is used by the proxy as input to the re-encryption function, which is executed by the proxy to translate cipher texts to the delegated user's key. Asymmertic proxy re-encryption schemes come in bi-directional uni-directional varities. Proxy re-encryption schemes allow for a cipher text to be re-encrypted an unlimited number of times. Proxy re-encryption should not be confused with proxy signatures, which is a separate construction with a different purpose.

Fig 4.Treatment History Details

6. Conclusion

Thus the development of cloud architecture for maintaining the personal health record and provide symptoms based treatment. The details of a patient are stored in a secured manner by applying proxy re-encryption method. A secured threshold proxy re-encryption server and integrates it with a decentralized erasure code such that a secure distributed storage system. Thus the proposed system improves the secured data in cloud and provides the treatment to the patient.

7. *References*

1. Hur. J, (2013) ' Improving Security and Efficiency in Attribute-Based Data Sharing',IEEETrans.Knowledge and Data Engineering, Vol.25,No.10.
2. Lai. J, Deng.R.H, Guan.C, and Weng.J ,(2013),'Attribute-Based Encryption Wieh Verifiable Outsourced Decryption',IEEETrans.InformationFortensics and Security ,Vol.8,No.8.
3. Li.M,YU.S,Cao.N and Lou.W,(2011)'Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing',Proc.31st Int'l Conf.Distributed Computing Systems.(ICDCS'11).

4. Li.M,Yu.S,Ren.k, and Lou.w, (2010)'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.

5. Li.M,Yu.S,Zheng.Y ,Ren.k, and Lou.w, (2013)'Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption',IEEETrans,Parallel and Distributed Systems,vol.24,No.1.

6. Lo''hr.H,Sadeghi.A.-R, and Winandy.M (2010) 'Securing the E-Health Cloud',Proc.First ACM Int'l Health Informatics Symp. (IHI '10),PP.220-229.

7. Michael Miller,"Cloud Computing Web Based Applications That Change the Way You Work and ColloborateOnline",QUE.

8. Nabeel.M, Shiang.N, and Bertino. E, (2013)'Privacy Preserving Policy-Based Content Sharing in Public Clouds',IEEETrans.Knowledge and Data Engineering,Vol.25,No.11.

9. Van Gorp. P, and Comuzzi .M, (2014) 'Lifelong Personal Health Data and Application Software via Virtual Machines in the Cloud',IEEE J. Biomedical and Health Informatics, Vol.18,No.1.

10. Yang. K, Jia. X, Ren.B,Zhang. K,Xie, R, (2013) 'DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems',IEEETrans.Information Forensics and Security,Vol.8,No.11.

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

12. Yu. S, Wang. C, Ren. K, and Lou. W, (2010),'Atrribute Based Data Sharing with Attribute Revocation',Proc,Fifth ACM Symp.Information,Computer and Comm.Security(ASIACCS'10).