Cloud Based Infirmary Monument

Archanaa M[1], Prasanna M[2] , Thiruselvan P[3]

**[1]IT Department, P.S.R.Rengasamy College of engineering for women,
Sivakasi -626140 , India**

**[2]IT Department, P.S.R.Rengasamy College of engineering for women,
Sivakasi -626140 , India**

**[3]IT Department, P.S.R.Rengasamy College of engineering for women,
Sivakasi -626140 , India**

Abstract

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In this paper we focus on systems that can support health care in the very challenging impoverished environments where the vast majority of the world’s population lives. With Cloud Computing data will be hosted in the Internet and medical staff can access it wherever and whenever they need it. We also present a number of challenging issues including reliable patient identification, data quality management, and data confidentiality and security, on line chatting between doctors, Online Blood bank maintenance and SMS service to the patient.Our software has the facility to give a unique id for every patient and stores the details of every patient and the staff automatically.Access to email or web communications allows staff to seek specialist advice from remote physicians.

Keywords: *cloud computing, Personal Health Record (EHR),*

1.Introduction

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or Provided by third-party service providers, for example, Microsoft HealthVault.1 Recently, architectures of storing PHRs in cloud computing have been proposed.

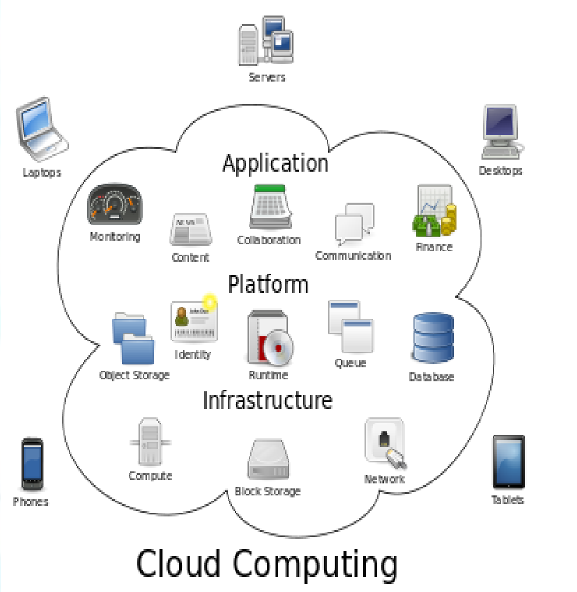


Fig: 1 Architecture of cloud

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi trusted servers. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the

PHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users.

Patients' data in an electronic format suppose several advantages such as greater data recording and improvement of QoS. Moreover, combining the Electronic Health Records (EHRs) with the Cloud Computing paradigm will improve these advantages. But first it's interesting to introduce the concept of Cloud Computing. With Cloud Computing a third-company provides the storage of the data in its servers and the maintenance of the system. So now users are going to get their resources and data from the net. That fact means that the customer just hires the services he needs, which implies economical savings for the management of the electronic resources. In order to get the best efficiency the Health Organism must evaluate all the available options to make the process of outsourcing of his data.

2. Architecture

Data confidentiality, unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents. On-demand revocation. Whenever a user's attribute is no longer valid, the user should not be able to access. Future PHR files using that attribute. This is usually called attribute revocation, and the corresponding security property is forward secrecy. There is also user revocation, where all of a user's access privileges are revoked. We shall prevent the unauthorized contributors to gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability. The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios. The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability. To deploy a Cloud Computing solution the size of the medical center and the amount of data that is going to be Transferred to the Cloud must be taken into account, so that
Just hire the necessary services. If in the future more services are needed, medical centers just have to contact with the Cloud provider and increase those resources. This information will be obtained knowing how many EHRs handle each center and the size of each EHR.

2.1. Problem Definition

We consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to the doctors and 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.

A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure) an open-source PHR system. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way.

2.2 Security Model

In this paper, we consider the server to be semi-trusted, i.e., honest but curious. That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

2.3 Requirements

To achieve "*patient-centric*" PHR sharing, a core requirement is that each patient can control who are authorized to access to her own PHR documents. Especially, user-controlled read/write access and revocation are the two core security objectives for any electronic health record system. The security and performance requirements are summarized as follows:

- *Data confidentiality*. Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

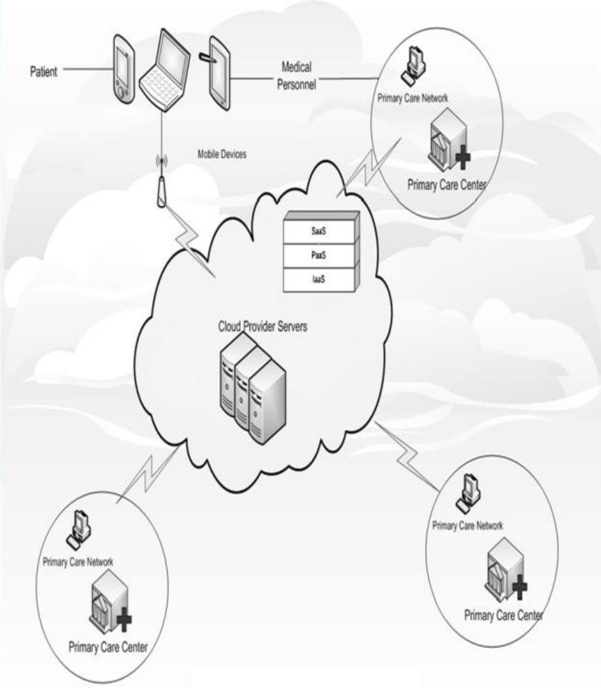
- *On-demand revocation*. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called *attribute revocation*, and the corresponding security property is forward secrecy. There is also *user revocation*, where all of a user's access privileges are revoked.

- *Write access control*. We shall prevent the unauthorized contributors to gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability.The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

- *Scalability, efficiency and usability*. The PHR system should support users from both the personal do-main and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

3. Overview of Our Framework

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.



4. Existing system

Existing system refers to the system that is being followed till now. Presently all the hospital functionalities are done manually. That is if a patient want to consult a doctor he can visit their till his chance called. This is making the person very difficult. Outpatient and In-patient tickets are distributed directly. The main disadvantage is time consuming.

4.1Draw Backs:

It has fewer modules for management process and poor security, Consumes large volume of paper work. Manual work No direct role for the higher officials. Any updating or changes can't be done. It's time consuming process and need time to change code for later updation process.

4.2Proposed system

The proposed system used for cloud based infirmary monument has layout structure that can process step by step. The employees in the hospital are given with a username for login which would be created by the admin along with the access level for security reason. The proposed system is a dynamic, which means the admin has full control for adding, viewing, deleting and updating of hospital information and creating new users and modules. The proposed system is Web-based so patients and healthcare providers can access it from any location. Moreover the architecture is cloud-based so large amount of data can be stored without any restrictions. Also the use of cloud computing architecture will allow consumers to address the challenge of sharing medical data that is overly comple and highly expensive to address with traditional technologies. This method will be also suitable in the Emergency Medical System (EMS) in order to improve the agility and coordination between the different emergency care processes. Several examples of Cloud-based solutions on e-Health services will be quoted in order to show that a lot of Health Organisms hire these solutions to improve the services they provide to their patients and the efficiency of their workers.

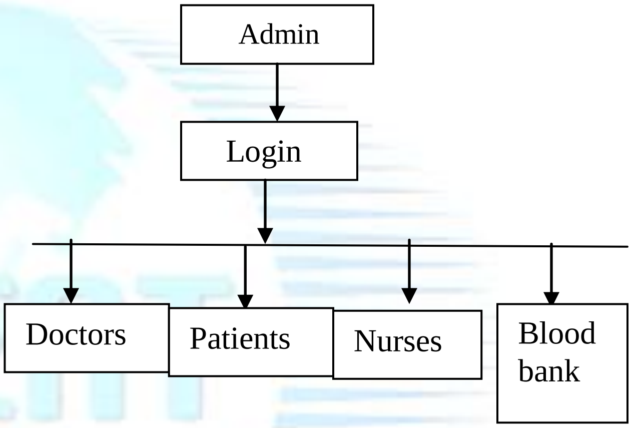
Goal**:**

Our goal is to assist healthcare providers in the adoption of PHR software and in the optimization of their clinical and practice management functions.

ADMIN MODULES

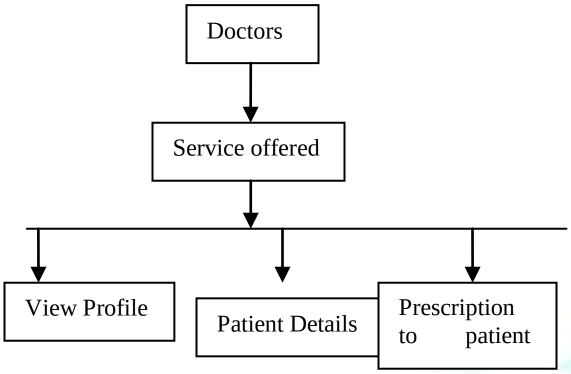
ADMIN is responsible for creating new login for employees, adding information about the hospital, doctors, nurse, patients, pharmacy, blood banks and monitors all activities in each modules.

ADMIN – is responsible for creating an access level for each employee in hospital for security reasons and explain the task needed to be performed by each employee. The medical staff will be able to access the EHRs through two different ways: Via the Hospital network which will be used by the medical staff during their working days and via Internet with any mobile device with Internet connection. The patient will access his medical records using credentials from these devices.



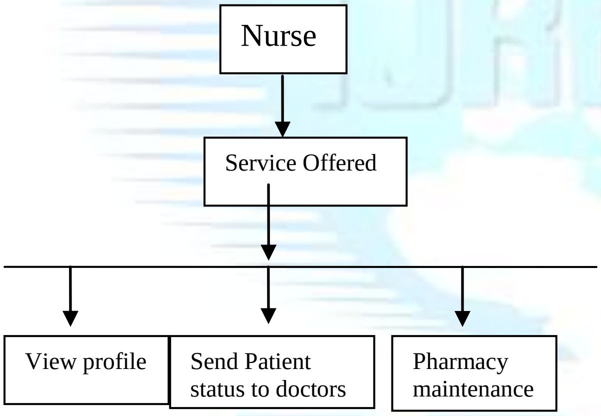
DOCTORS MODULES

In these modules a doctor can view his profile, salary details and view his patient's health status and prepare a medical prescription and send to the nurse for future process about patient's health.



NURSE MODULES

In these modules a nurse can view his profile, salary details and get medical prescription from a doctor and send health status of patients to the doctor.

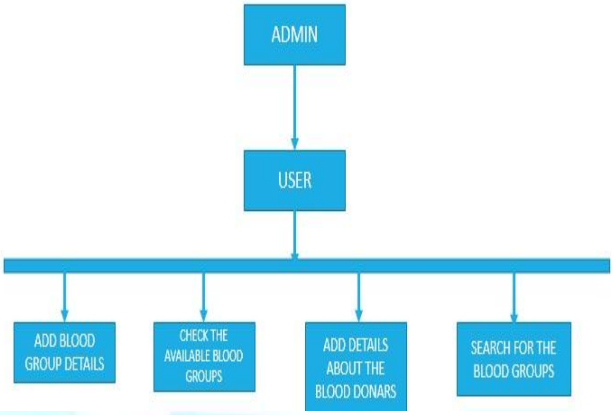


PHARMACY MODULES

In this modules admin add details about the medicines available in the pharmacy and create a user for managing pharmacy details like bill payments, medicine transaction etc.

BLOOD BANK MODULES

In these modules admin add details about the available blood groups and details about the persons who donated the bloods.To create electronic blood donor management information system in order to assist in the management of blood donor records, planning and share information in a more confidential, convenient and secure way using modern technology.


ADMIN
USER
ADD BLOOD GROUP DETAILS
CHECK THE AVAILABLE BLOOD GROUPS
ADD DETAILS ABOUT THE BLOOD DONARS
SEARCH FOR THE BLOOD GROUPS

HARDWARE REQUIREMENTS

• Processor Name	:	Dual Core
• Processor Speed	:	3.2 GHz
• RAM	:	1 GB
• Hard Disk Capacity	:	80 GB
• Display Device	:	14' to 19' Inch Monitor
• Keyboard Type	:	PS2 or USB
• Mouse Type	:	PS2 or USB

SOFTWARE REQUIREMENTS

• Technology Implemented	:	Dream weaver
• Language Used	:	PHP 5.2
• Database	:	My SQL 5.2
• User Interface Design	:	HTML, AJAX
• Web Browser	:	Mozilla,IE8

CONCLUSION

In the proposed system, we have proposed a novel 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.

REFERENCES-

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter. Patient controlled encryption: ensuring privacy of electronic medical records. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, 2009. Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville,R., and Taylor, R., Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. Heal. Aff. 24:1103–1117, 2005.

[2]. Blanchet, K. D., Electronic health records: Are consumers ridingor driving the car? Telemed. E-health 14:210–214, 2008.

[3]. Yellowlees, P. M., Marks, L. S., Hogarth, M., and Turner, S.,Standards-based, open-source electronic health record systems: A desirable future for the U.S. Health Industry. Telemed. E-health 14:284–288, 2008.

[4]. Hargreaves, J., Will electronic personal health records benefit providers and patients in Rural America? Telemed. E-health 16:167–176, 2010.

[5]. Chen, Y. Y., Lu, J. C., and Jan, J. K., A secure EHR system based onhybrid clouds. J. Med. Syst., 2012. doi:10.1007/s10916-012-9830-6.

[6]. Furth, B., Escalante, A., Handbook of cloud computing 1st Edition. Springer, 2010.

[7]. Low, C., and Chen, Y. H., Criteria for the evaluation of a Cloud-Based Hospital Information System Outsourcing Provider. J. Med.Syst., 2012. doi:10.1007/s10916-012-9829-z.

[8]. Poulymenopoulou, M., Malamateniou, F., and Vassilacopoulos.G., Emergency healthcare process automation using mobile computingand cloud services. J. Med. Syst., 2011.