Mobile HealthCare Monitoring System in Mobile Cloud Computing

D.Hari Prasad¹, M.Srikanth²

¹M.Tech (CSE) II Year Student, Prasad Engineering College, Jangon, Warangal, Telangana State.
²Associate Professor, Department of CSE, Prasad Engineering College, Jangon, Warangal, Telangana State.

E-mail: hariprasad.dindigala@gmail.com

Abstract

Cloud computing is on-demand computing that does not reside at the users’ premise. Instead of the computing resources are owned and managed by a cloud service provider and the user’s access the resources via the Internet. Cloud-Assisted m(Mobile)-Health Care Monitoring System, it concern the current promising areas Mobile Communications and Cloud Computing Technologies to provide feedback, decision support, has been considered as a revolutionary approach to improving quality of health care services while lowering the health care cost. Unfortunately, it also cause a serious risk on both patients or clients privacy and intellectual property of monitoring service providers, which could deter the wide adoption of m-Health Care technology. This paper is explore this particular important problem and to design and implement a Cloud-Assisted Privacy preserving m (Mobile) Health Monitoring System to protect the privacy of the involved stakeholders and their sensitive and critical data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved stakeholders to the cloud without compromising patients or clients’ privacy and service providers’ intellectual property.

1. INTRODUCTION

Cloud Computing is no more considered as an emerging technology. Now, it’s a reality and this low-cost computing power is gaining popularity among businessmen, especially medium and small size, and public (government) organizations, as people are realizing the power of cloud environments. Cloud computing is such a type of computing environment, where business owners outsource their computing needs including application software services to a third party and when they need to use the computing power or employees need to use the application resources like database, email, etc., they access the resources via internet.

Mobile technology has expanded dramatically around the world. Along with 3G and 4G, these advances have had a huge impact on many walks of life. The utilization of smart phones and tablets has transformed communications, commerce, and gaming, among other related fields. Their emergence has improved service delivery, empowered consumers, businesses, and entrepreneurs, and changed the way in which people access information and make transactions. Now this technology is composed to alter how health care is delivered, the quality of the patient experience, and the cost of health care. Mobile technology is helping with chronic disease management, extending service to underserved areas, and improving health outcomes and medical system efficiency.

Mobile phones as a service platform can provide several societal, business and governmental services. Further developments will allow mobile devices with unique features that can sense the environment and physiological parameters to enhance quality of life and remote monitoring of patients. However mobile devices have limitations in computational capacity and power consumption. Hence, cloud computing could be regarded as an unlimited resource that can be accessed anytime and anywhere in the world.

2. RELATED WORK

The mobile health service is provided by the mobile health providers. The provider gives the facility of health monitoring according to patient’s convenience with the maximum use of mobile device. The client who wants to use this application subscribes to the mobile health provider through his mobile. The providers register them as authenticated user after validation of information. The further communication is done through the mobile only.

Monitoring devices enable patients with serious problems to record their own health measures and send them electronically to physicians or specialists. This keeps them out of doctor’s offices for routine care, and thereby helps to reduce health care costs. The chronic

Disease areas are congestive heart failure, pulmonary disease, diabetes, and skin ulcers. With around the clock monitoring and electronic data transition to caregivers, remote devices speed up the treatment of patients requiring medical intervention. Rather than having to wait for a patient to discover there is a problem, monitors identify deteriorating conditions in real-time, and alert physicians. For example, Cloud-Assisted Mobile (Mobile)-Health Care Monitoring System, it concern the current promising areas Mobile Communications and Cloud Computing Technologies to provide feedback, decision support, has been considered as a revolutionary approach to improving quality of health care services while lowering the health care cost. Unfortunately, it also cause a serious risk on both patients or clients privacy and intellectual property of monitoring service providers, which could deter the wide adoption of m-Health Care technology.

This paper pragmatically demonstrate this particular important problem and to design and implement a Cloud-Assisted Privacy Preserving m (Mobile) Health Monitoring System to protect the privacy of the involved stakeholders and their sensitive and critical data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re-encryption are adapted to shift the computational complexity of the involved stakeholders to the cloud without compromising patients or clients’ privacy and service providers’ intellectual property. Finally, the outcome is the security and performance analysis demonstrates the effectiveness of proposed system design and implementation.

3. PROPOSED WORK

The main aim of this paper is to implement a mobile internet application in the cloud environment for health care monitoring system for the hospital allied applications, in which the patients can download the hospital management system software and also able to get appointment form the corresponding doctors and also able to view basic symptoms and immediate first aids to be taken.

We could also consider autonomic computing issues, which defines a set of architectural characteristics to manage systems where complexity is increasing but must be managed without increasing costs or the size of the management team, where a system must be quickly adaptable to new technologies integrated to it, and where a system must be extensible from within a corporation out to the broader ecosystem and vice versa. CAM (cloud assisted mobile) consists of four parties: the cloud server (simply the cloud), the company who provides the mHealth monitoring service (i.e., the healthcare service provider), and the individual clients (simply clients), and a semi-trusted authority (TA). The company stores its encrypted monitoring data or program in the cloud server. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud server through a mobile (or smart) device. A semi-trusted authority is responsible for distributing private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client input vectors.

4. SYSTEM ARCHITECTURE

Figure 1. Patient (client) and Cloud (server)

The proposed system architecture for developing and deploying the mobile healthcare applications that utilize Cloud computing. The Cloud service client consists of several modules. The Patient health record application acquires and displays patient records stored into the cloud. The Cloud storage Facilities manages the physical infrastructure (e.g., storage elements) and is also responsible for performing maintaining operations (e.g., backup critical data, etc.) The Cloud platform interface is also connected to the Cloud service module, which handles and queues user requests. The patient is the client who uses this application. The client who wants to use this has to subscribe to the administrator and send the necessary documents for the registration. The administrator is the person who has the medical background. Whenever the
client sends the request for registration the administrator first verify the necessary documents and register him as the authorized customer with the unique PatientID. The client can access the data in the cloud storage but can’t do the modification in the record.

The security purpose the administrator only has the rights to make the changes in the record. The registered customers have their accounts with unique ID and password. These accounts are managed by the administrator. He has the backup of all information related to these account Cloud provides the storage for patient record. Send the data to the client when request is generated.

5. APPLICATIONS OF m-HEALTH CARE

There are a few schemes of Mobile Cloud Computing applications in healthcare. For example, [5] presents five main mobile healthcare applications in the pervasive environment.

a. Comprehensive Health Monitoring Services: This enable patient to be monitored at anytime and anywhere through broadband wireless communications.

b. Intelligent Emergency Management System: It can manage and coordinate the fleet of emergency vehicles effectively and in time when receiving calls from accidents or incidents.

c. Health-Aware Mobile Devices: It could detect pulse-rate, blood pressure, and level of alcohol to alert healthcare emergency system.

d. Pervasive Access to Healthcare: This critical information allows patients or healthcare providers to access the current and past medical information.

e. Pervasive Lifestyle Incentive Management: It can be used to pay healthcare expenses and manage other related charges automatically.

6. IMPLEMENTATION

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. Many software applications, services, and data once in the domain of a local computer or local server safely secure in your building are now in the domain of the public interest. Private health information once confined to these local networks is migrating, wholesale, onto the internet. Patients voluntarily grant access to their health records every time they sign a contract to the health insurer that then decides on the payment disposition to the doctor, pharmacy, or hospital. For the most part, the collection and organization of this data is completely legal.

7. SECURITY AND PRIVACY ISSUES

Providing access to browser-based or mobile client’s and devices with end-to-end encryption in either:

- Tightly controlled private clouds.
- Non-private clouds only if the patient identifiers are stored in encrypted data files (in the cloud storage).
- Storing de-identified patient critical data in centralized database for public access or for restricted access by authorized administrator.
- Mobile applications in private clouds with end-to-end encryption.
- Hosting web conferences to dispersed audiences.
- Enabling real-time collaboration in private clouds with patient data encrypted end-to-end or in public clouds with de-identified patient data only.

The Mobile health care (m-HealthCare) monitoring system can greatly improve the benefits for patients and hospitals, by not only providing better quality of patient care, but by also reducing administrative and medical cost for both patients and hospitals.

8. FUTURE SCOPE

Future scope of work could include and improving security and privacy is strengthen by implementing advanced user authentication techniques on the mobile device and deploying the platform in practical and real world public healthcare environment for evaluating the
system in terms of user acceptability and performance. The integration and security related issues can still be considered for the future work in order for the more secure and easy, efficient integration and use of the upcoming components and current technology.

References


