ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 7 , July 2017

Privacy Preserving Mechanism for Mobile Healthcare Emergency

SOFIYA T, Dr. CHETANA PRAKASH

PG student, Department of computer science and engineering, Bapuji Institute of Technology, Davanagere, Karnataka
Head, Department of MCA, Bapuji Institute of Technology, Davanagere, Karnataka, India.

ABSTRACT: The following decade will witness a surge in remote health-monitoring systems that are based on body-worn monitoring devices. These Medical Cyber Physical Systems (MCPS) will be capable of transmitting the acquired data to a private or public cloud for storage and processing. Machine learning algorithms running in the cloud and processing this data can provide decision support to healthcare professionals. There is no doubt that the security and privacy of the medical data is one of the most important concerns in designing an MCPS. The pervasiveness of smart phones and the advance of wireless body sensor networks (BSNs), mobile Healthcare (m-Healthcare), which extends the operation of Healthcare provider into a pervasive environment for better health monitoring, has attracted considerable interest recently. However, the flourish of m-Healthcare still faces many challenges including information security and privacy preservation.

KEYWORDS: Medical Cyber Physical Systems, Medical Data Privacy, Body sensor Networks, Mobile Healthcare.

I. INTRODUCTION

Proposed system goes for the security and protection issues, and builds up a user driven security get to control of opportunistic registering in m-healthcare emergency. The application records various physiological signs such as pulse rate, body temperature, blood sugar and blood pressure of the patient. We propose a protected and security safeguarding framework called Medical Cyber Physical Systems (MCPS) for m-Healthcare emergency [5].The advancement of devices empowered the improvement of these devices that is clinically utilized. The patient's health information is obtained and transmitted over cloud. Patient medical data is encrypted by using AES schemes to provide data privacy during transmission. Results will be provides from the encrypted data by the doctor.

Move from a clinically oriented, brought together medicinal services framework to a patient situated, appropriated human services framework. Diminish healthcare costs through more productive utilization of clinical assets and prior recognition of medicinal conditions challenges [4]. While the traditional encryption plans were giving just secure storage option, emerging encryption plans also provides secure information sharing and computation. Assuring the privacy of patient's health details during the transmission from mobile application to server and from server to doctor's web application. Decision support is facilitated in cloud for healthcare experts by applying critical system to the procured information and anticipating patient health condition [2].

Definite security examination demonstrates that the proposed system can effectively accomplish user driven protection get to control in m-Healthcare crisis. Also, execution assessments by means of extensive simulations show the viability in term of giving high reliable personal health data process and transmission while limiting the protection disclosure amid m-Healthcare emergency [6].Designing MCPS requires upcoming technological obstacles in establishing the architectural parts of the MCPS and assuring the privacy of patient's health details during the transmission from mobile application to server and from server to doctor's web application. This also involves encryption scheme such as AES to give secure capacity, secure information sharing and computation.

As indicated by the Health Insurance Portability and Accountability Act (HIPAA),Information security must be ensured within each layer of a MCPS [1]. Some of the encryption plans guarantee that medicinal information is

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 7 , July 2017

assessed only by approved users, in this manner giving information protection on confined information squares. Guaranteeing framework level protection requires laying out a crypto-outline for the MCPS all things considered.Because of the distinctions in hardware and communication capacities of every layer, assorted encryption plans should be utilized to ensure information protection inside that layer in perspective of their capacity to give secure capacity, information sharing and computation in a MCPS.

II SYSTEM ANALYSIS

Analysis phase is a detailed study of various operations performed by a system and their relationships within and outside the system. One aspect of system analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related systems. The emphasis in system analysis is on identifying what is needed from the system and not how the system will achieve its goal.

1 Existing system

In Existing System, According to the senses over the age of 65 is expected to hit 70 million by 2030, having doubled since 2000. Health care expenditures projected to rise to 15.9% by 2010 [7]. The cost of health care for the nation's aging population has become a national concern are important for understanding how the opportunistic computing paradigm work when resources available on different nodes can be opportunistically gathered together to provide richer functionality, they have not considered the potential security and privacy issues existing in the opportunistic computing paradigm.

2Proposed System

In our proposed SPOC (Secure and Privacy-preserving Opportunistic Computing Framework) aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m- Healthcare emergency. For example, as shown in Fig.2.1, each mobile medical user's personal health information (PHI) such as heart beat, blood sugar level, blood pressure and temperature and others, can be first collected by BSN, and then aggregated by smartphone via Bluetooth. Finally, they are further transmitted to the remote healthcare center via 3G networks. Based on these collected PHI data, medical professionals at healthcare centre can continuously monitor medical users' health conditions and as well quickly react to users' life-threatening situations and save their lives by dispatching ambulance and medical personnel to an emergency location in a timely fashion.

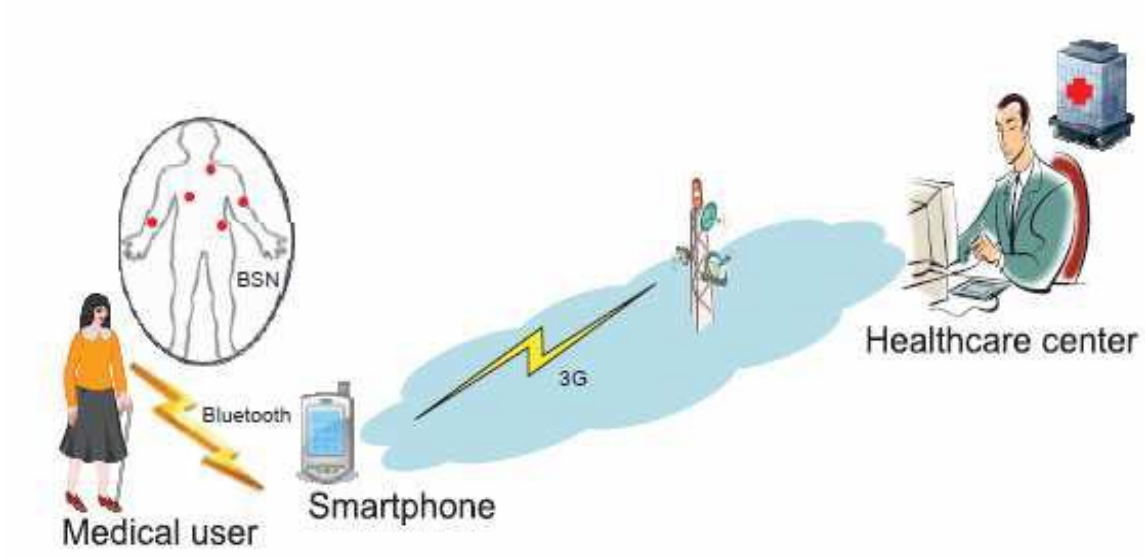


Fig 2.1: SPOC framework for mobile healthcare emergency

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 7 , July 2017

The functional requirements of the system are:

- Admin can add, edit and delete the locations. They can create/add the trusted authority users in one Location. They can do the Edit, View and Delete the same (Users details). They can able to view the patients who are needs help. Admin can change the password of the admin user. After adding the trusted user in one location the login credential will be available for the trusted users.

- Authorized users (who are added in admin module) only can login. The Authorized Users can add/create the patients and their details in the application. Also they can view all registered patient details and single registered users at the same time. The purpose of viewing single patient detail is nothing but who are in under critical condition they are visible primarily for Authorized users. The authorized user sends the SMS (about patient condition) who are registered in the patient's profile. A user can change the password is also possible. The critical condition factors of patient is patient temperature, Blood pressure, Sugar etc.,

- The patients or clients have the login facility. If they feel their health condition to be monitored by the authorized users then it is possible. The patients can able view their health conditions certainly. They use the map facility in their device for various needs. If the patient feels unsafe condition they can send the information to authorized users. Finally they can modify the password also not an issues.

Advantages:

- Shift from a clinic-oriented, centralized healthcare system to a patient oriented, distributed healthcare system.
- Reduce healthcare expenses through more efficient use of clinical resources and earlier detection of medical conditions Challenges.
- Performance, Reliability, Scalability, QoS, Privacy, Security …

III DATA PRIVACY USING CONVENTIONAL ENCRYPTION SCHEME

In this section, we study the conventional AES encryption scheme, which can only guarantee data privacy. However, this is widely used due to their substantially lower resource requirements as compared to emerging schemes.

1 Advanced Encryption Standard (AES)
AES is one of the most widely used symmetric key encryption algorithms and is accepted as an industry and a government applications standard. AES is optimized for speed, low memory footprint and energy efficiency. Its low resource intensity allows AES to run on a wide range of hardware platforms ranging from 8-bit microcontrollers to high-end desktops and servers.

Algorithm: AES Encryption

input : Plaintext Block ptxtb, Secret Key sk
output: AES state state
state = InitState(ptxtb, sk)
AddKey(state, sk0)
for i = 1 **to** nr _ 1 **do**
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddKey(state, keyi)
SubBytes(state)
ShiftRows(state)
AddKey(state, keynr_1)

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 7 , July 2017

IV. DIAGRAMMATIC REPRESENTATION

Fig 4.1 shows diagrammatic representation of the system. The project target MCPS is a remote patient health monitoring system that transmits patient blood pressure, heart rate etc., from the patient's house into the cloud. Patient medical data is thought to be encrypted using AES encryption technique to give information privacy during transmission. Encrypted patient data will give certain insights and discovery results to the specialist. The objective of this application is to continuously screen a patient's heartbeats and alert the doctor when surpasses a clinical limit.

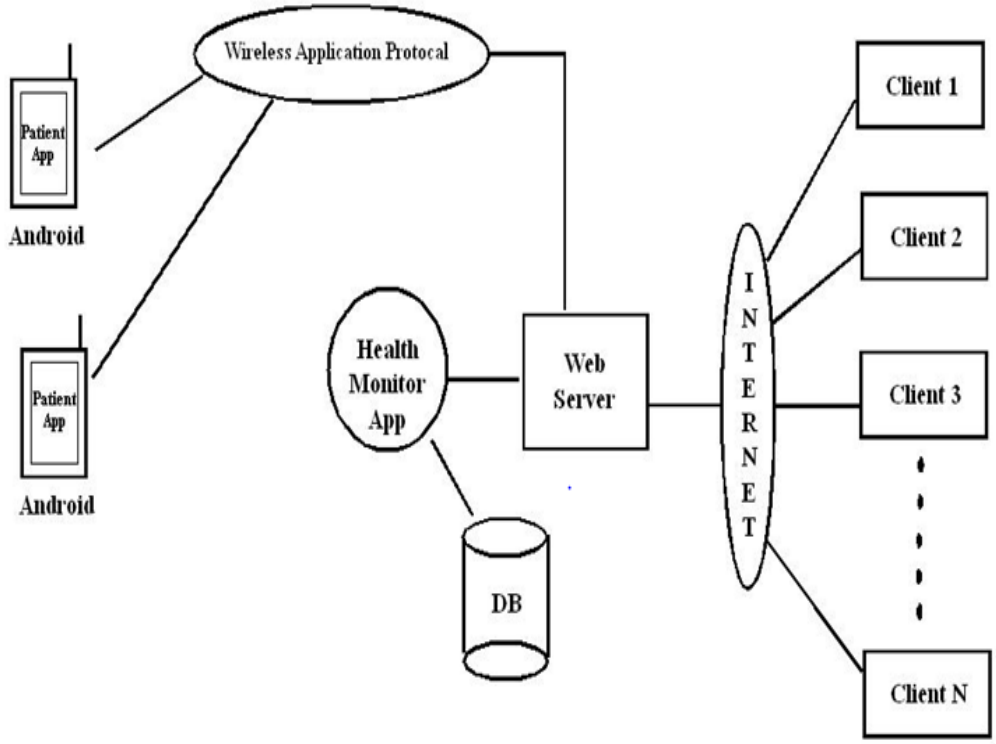


Fig. 4.1 Diagramatic representation.

V TESTING OF SYSTEM

A primary purpose of testing is to detect software failures so that defects may be discovered and corrected. This is a non-trivial pursuit. Testing cannot establish that a product functions properly under all conditions but can only establish that it does not function properly under specific conditions. The scope of software testing often includes examination of code as well as execution of that code in various environments and conditions as well as examining the aspects of code: does it do what it is supposed to do and do what it needs to do

System Testing is a set of activities that can be planned in advance and conducted systematically. The proposed system is tested in parallel with the software that consists of its own phases of its analysis, implementation, testing and maintenance.

A unit is the smallest testable part of an application. During this implementation of the system each module of the system was tested separately to uncover errors within its boundaries. User interface is used as a guide in the process. In

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 7 , July 2017

computer programming, unit testing is a method by which individual units of source code are tested to determine if they are fit for use.

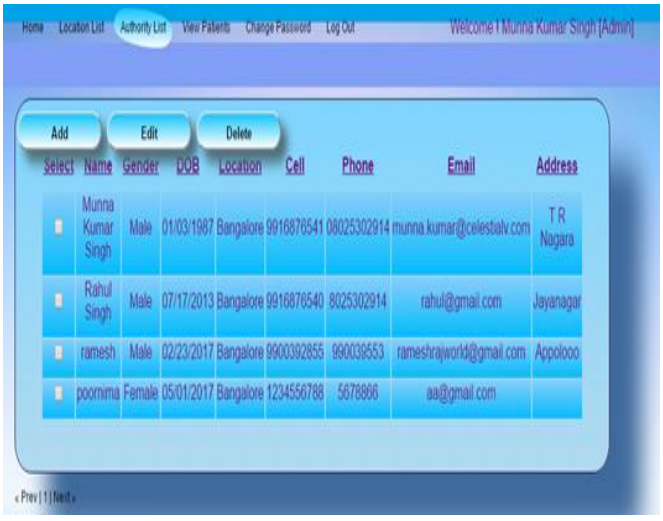
A module is composed of various programs related to that module. Module testing is done to check the module functionality and interaction between units within a module. It checks the functionality of each program with relation to other programs within the same module. It then test the overall functionality of each module. This module introduces the technique of functional (blackbox) unit testing to verify the correctness of classes. It shows how to design unit test cases based on a class specification within a contract programming approach.

Integration testing is a systematic technique for constructing the program structure while conducting tests to uncover errors associated with interfacing. The object is to take unit tester module and build a program structure that has been dictated by the design.

Acceptance testing generally involves running a suite of tests on the completed system. Each individual test, known as a case, exercises a particular operating condition of the user's environment or feature of the system, and will result in a pass or fail, or boolean outcome.

VI. RESULTS

In Fig 6.1 a) Authority list which is created by admin. b) Patients readings, where patient locality and health details are only visible for authorized users. If the patient/client doesn't want to be monitored by the other person then they can disable the system. c) Ambulance list, if the patient is in critical health condition or the patient feels abnormal condition then the authorized users can gives the first aidand also will send the SMS to ambulance driver to pick up the patient. d) Data monitoring page where patient send their details through the application.



a)

b)

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 7 , July 2017

c) d)

Fig. 6.1: a) Authority Creation page b) Patient readings c) Ambulance list d) Data monitoring Page

VII. CONCLUSION

The purpose of this project is to save the life of critical stage patients and the authorized user can able to monitor the patient's details and their health condition continuously. Patient locality and health details are only visible for authorized users. If the patient is in critical health condition or the patient feels abnormal condition then the authorized users can gives the first aid, send the SMS to their relatives, and Authorized user will send the SMS to ambulance driver to pick up the patient. Secure computation and storage requirements provided using AES encryption. The decision support is facilitated for healthcare professionals by applying critical system to acquired data and predicting patient health condition.

VII. SCOPE

In future this application can be enhanced by using sensors. From the sensors patient's data will be collected and will give to the trusted authority to predict the health condition of the patient.

REFERENCES

[1] N. Powers, A. Alling, K. Osolinsky, T. Soyata, M. Zhu, H. Wang, H. Ba, W. Heinzelman, J. Shi, and M. Kwon, "The cloudlet accelerator: Bringing mobile-cloud face recognition into realtime," in Globecom Workshops (GC Wkshps), Dec 2015

[2] A. F. Hani, I. V. Paputungan, M. F. Hassan, V. S. Asirvadam, and M. Daharus, "Development of private cloud storage for medical image research data," in Int. Conf. on Computer and Inf. Sciences (ICCOINS), June 2014, pp. 1–6.

[3] S. X. et al., "Soft microfluidic assemblies of sensors, circuits, and radios for the skin," Science, vol. 344, pp. 70–74, 2014.

[4] A. Page, O. Kocabas, T. Soyata, M. K. Aktas, and J. Couderc, "Cloud-Based Privacy-Preserving Remote ECG Monitoring and Surveillance," Annals of NoninvasiveElectrocardiology (ANEC), vol. 20, no. 4, pp. 328–337, 2014.

[5] A. Benharref and M. A. Serhani, "Novel cloud and SOA-based framework for E-Health monitoring using wireless biosensors," IEEE Journal of Biomed. and Health Inf., vol. 18, no. 1, pp. 46–55, Jan 2014.

[6] S. Babu, M. Chandini, P. Lavanya, K. Ganapathy, and V. Vaidehi, "Cloud-enabled remote health monitoring system," in Int. Conf. on Recent Trends in Inform. Tech. (ICRTIT), July 2013, pp. 702–707.

[7] D. Kim, R. Ghaffari, N. Lu, and J. A. Rogers, "Flexible and stretchable electronics for biointegrated devices," Annual Review of Biomedical Engineering, pp. 113–128, 2012.

[8] T. Soyata, R. Muraleedharan,C. Funai, M. Kwon, and W. Heinzelman, "Cloud-Vision: Real-Time Face Recognition Using a Mobile-Cloudlet-Cloud Acceleration Architecture," in IEEE Symposium on Computers and Communications, Jul 2012, pp. 59–66.

[9] Y. Mao, Y. Chen, G. Hackmann, M. Chen, C. Lu, M. Kollef, and T. C. Bailey, "Medical data mining for early deterioration warning in general hospital wards," in IEEE 11th Int. Conf. on Data Mining Workshops (ICDMW), Dec 2011, pp. 1042–1049.

[10] A. Pantelopoulos and N. G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis," IEEE Trans. Sys., Man, and Cybernetics, Part C: Applic, and Reviews, vol. 40, no. 1, pp. 1–12, Jan 2010.