# An Implementation for secure Mobile-Healthcare framework using Android App Development Environment

Bharat Bhushan Singhal[1], Mr. Dushyant singh[2]
[1]First Author M.TECH(CSE) student at Rajasthan Technical University,Kota,Rajasthan
[2]Second Author Assistant Professor at Chandrawati Group of Institution, Bharatpur,Rajasthan.

## Abstract

In today s world rate of accident is very high, if the victim is not treated properly on time then there is chance that he loses his life and as life is very precious to every human being and hence this has motivated us to do a project. Doctors play a very important role in daily life, if a person falls ill then first he consult a doctor and if doctor is not available then it is creates a lot of problem to the patient and his livelihood will be disturbed. A very well-known proverb says- health is wealth . As we know m-hospital is common now a days but it provide only few features like checking BP and providing medicine for disease like cold etc. But our project provides better first aid and even sees to it that patients get diagnosed as early as possible and even take the patients to the nearby hospital and give emergency aid to them.

**Key Words:** m-healthcare,BSN

## I. Introduction

Mobile Healthcare is one of the advanced technologies of the 21st century. It can be used to provide auxiliary medical services and has accordingly been used in emergency situations, mobile hospitals, personal healthcare, and in rapidly alerting doctors to a patients condition, etc. By exploiting the advantages of wireless multimedia communication, such as current high utility, convenience, high data transmission rates, high the accident victim to the emergency clinic. This enables the physician in the clinic to assess the patient s physiological condition in advance and arrange for emergency medical resources well in time, which could decrease the actual time required for treating the patient.

Although m-Healthcare system can benefit medical users by providing high-quality pervasive healthcare monitoring, the flourish of m-Healthcare system still hinges upon how we fully understand and manage the challenges facing in m- Healthcare system, especially during a medical emergency. To clearly illustrate the challenges in m-Healthcare emergency, we consider the following scenario. In general, a medical user s PHI should be reported to the healthcare center every 5 minutes for normal remote monitoring. However, when he has an emergency medical condition, for example, heart attack, his BSN becomes busy reading a variety of medical measures, such as heart rate, blood pressure, and as a result, a large amount of PHI data will be generated in a very short period of time, and they further should be reported every 10 seconds for high-intensive monitoring before ambulance and medical personnel s arrival. However, since smart phone is not only used for healthcare monitoring, but also for other applications, i.e., phoning with friends, the smart phone s energy could be insufficient when an emergency takes place. Although this kind of unexpected event may happen with very low probability, i.e., 0.005, for a medical emergency, when we take into 10, 000 emergency cases into consideration, the average event number will reach 50, which is not negligible and explicitly indicates the

reliability of m-Healthcare system is still challenging in emergency.

In our proposed framework aims at the security and privacy issues, and develops a user-centric privacy access control of opportunistic computing in m-Healthcare emergency. The application we designed is mainly used by any individual who owns a car. It acts like a basic aid at the time of emergency from a remote place. We have used GSM modem, instead it could be even worked with the satellite. Our application makes an attempt for a basic aid, it can be further extended by using various latest technologies like embedding machine and various other device these come at the cost of expense.

## II. Existing System

In Existing System, According to the sensex 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. 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. Also in the existing system hardware and J2Me Technology used which is very old system.

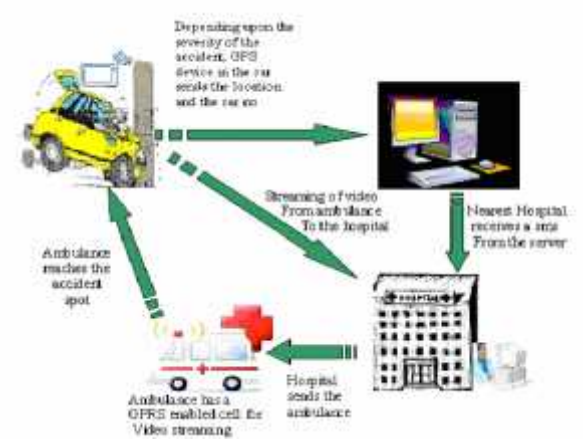



**Fig 2.1 Existing System**

Figure 2.1 describe about each module and tell what exactly each module do i.e. interaction between each module and how they connect each other.

But existing system have many drawback like

- its not up to date system
- Hardware is used which is vulnerable.
- GPS and GSM must be replaced.

So we have proposed new solution so that we can add new functionality to our system.

## III.Proposed System

Server Phase where the administrator has the right to Register a new Customer, Hospital. Receives Alert messages from Hospitals stating it has started working, Sms messages from where the accident has occurred. Send request for service for the hospitals and Ack the same.

Client(Hopital) Phase where the sends alert message to the Server Pc stating it ahas started working, and waits for the request from the serer PC, Once request is received then upon condition accept or reject it. Once accepted it will send an Alert message (response) to the Server and then recives the Response from server as a Ack.

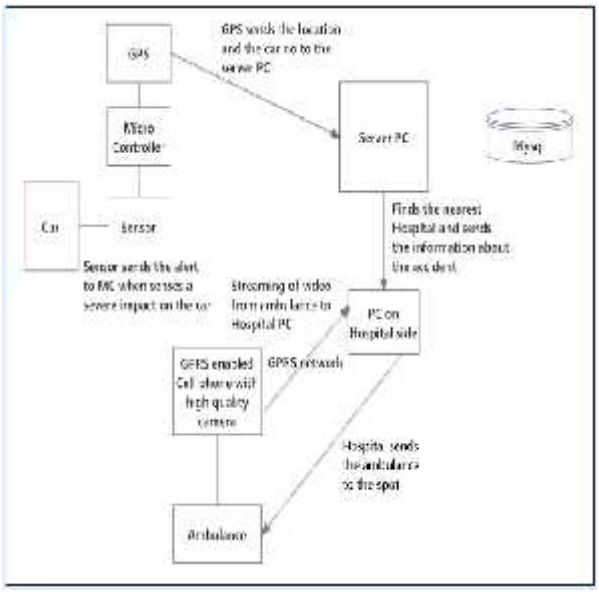



**Fig 3.1 Proposed System**

**Functional Requirements**

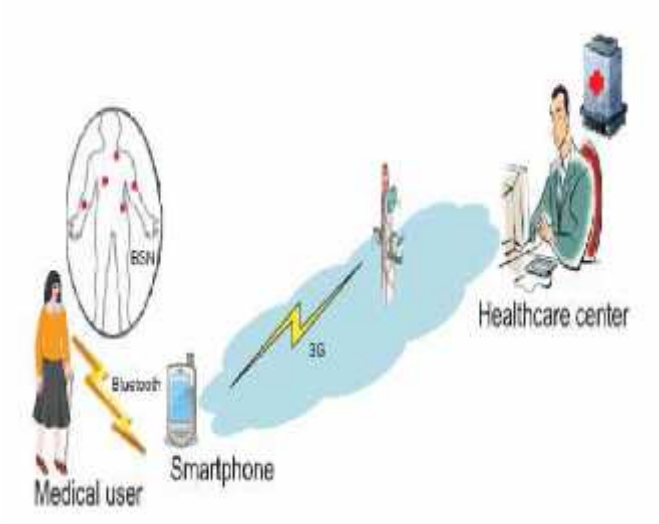
Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

- The Body Sensors have to measure the Human Body details such as Blood Sugar Level, Body Temperature, Blood Pressure, and Heart Beat etc.
- The Details will be sending to Health care Centre in secure way by using paillier cryptography techniques.
- The Health Care Centre receives the body sensed details and decrypting the same in HCC.
- The Healthcare Centre replies to remote patient by sending the ambulance details via Mobile device using PPSPC Protocol and the other conversation will be happening via mobile after admitting the patient in the specified hospital.
- The Attributes are Patient body sensor details,Security,Performance,BP,HB,SL,BT,HCC,Sensors,Backbone Router, Home Healthcare Gateway

**Modules and their description**

**1.Pervasive Health Monitoring in M-Healthcare(Server)**

In this module, 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 smart phone 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 center 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.




**2. Client**

In this module, Body area network (BAN), wireless body area network (WBAN) or body sensor network (BSN) are terms used to describe the application of wearable computing devices. This will enable wireless communication between several miniaturized body sensor units (BSU) and a single body central unit (BCU) worn at the human body.

Deploy wearable sensors on the bodies of patients in a residential setting

Continuously monitor physiological signals (such as ECG, blood oxygen levels) and other health related information (such as physical activity).

**ALGORITHM Server ()**

//Input: Longitude and latitude from telemedicine hardware.

//Output: Display the list of hospitals and acknowledge all the hospitals.

While (1)

{

Registration of vehicle and hospital by administrator;

n=validate();

if(n==false)

{

user has to enter his details once again ;

}

else

{

//Give unique number to all hospital;

For i ← 0 to number of hospitals

{

Hospital number=i+1;

}

*Step 5. Send reply ambulance details to the remote patient via Mobile device using PPSPC protocol.*

*Step 6. Process the query between Remote user and HCC via Hand Held Mobile Device*

## 3.Security Analysis

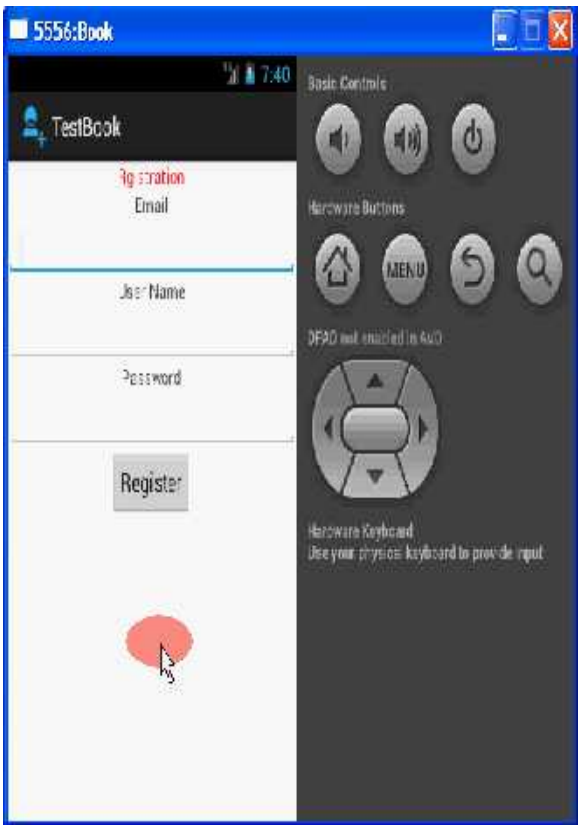
In this Module to develop a secure and privacy-preserving opportunistic computing framework to provide high reliability of PHI process and transmission while minimizing PHI privacy disclosure in m-Healthcare emergency. Specifically, we i) apply opportunistic computing in m-Healthcare emergency to achieve high-reliability of PHI process and transmission; and ii) develop user-centric privacy access control to minimize the PHI privacy disclosure.

### IV Implementation

RUN

1.Initially, first page of server

2. Login and Registration page in Android:




## V.Conclusion and Future Work

In this paper, we have proposed a secure and privacy preserving opportunistic computing framework for m-Healthcare emergency, which mainly exploits how to use opportunistic computing to achieve high reliability of PHI process and transmission in emergency while minimizing the privacy disclosure during the opportunistic computing. Detailed security analysis shows that the proposed framework can achieve the efficient user-centric privacy access control. In addition, through extensive performance evaluation, we have also demonstrated the proposed SPOC framework can balance the high-intensive PHI process and transmission and minimizing the PHI privacy disclosure in m-Healthcare emergency. In our future work, we intend to carry on smart phone based experiments to further verify the effectiveness of the proposed SPOC framework. In addition, we will also exploit the security issues of PPSPC with internal attackers, where the internal attackers will not honestly follow the protocol.

We have to use GSM modem, instead it could be even worked with the satellite. Our application makes an attempt for a basic aid, it can be further extended by using various latest technologies like embedding ECG machine and various other device these come at the cost of expense.

## References:

[1] A. Toninelli, R. Montanari, and A. Corradi, Enabling secure service discovery in mobile healthcare enterprise networks, IEEE Wireless Communications, vol. 16, pp. 24 32, 2009.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network, in Proc. BodyNets 10, Corfu Island, Greece, 2010.

[3] Y. Ren, R. W. N. Pazzi, and A. Boukerche, Monitoring patients via a secure and mobile healthcare system, IEEE Wireless Communications, vol. 17, pp. 59 65, 2010.

[4] R. Lu, X. Lin, X. Liang, and X. Shen, A secure handshake scheme with symptoms-matching for mhealthcare social network, MONET, vol. 16, no. 6, pp. 683 694, 2011.

[5] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption, IEEE Transactions on Parallel and Distributed System, to appear.

[6] M. R. Yuce, S. W. P. Ng, N. L. Myo, J. Y. Khan, and W. Liu, Wireless body sensor network using medical implant band, Journal of Medical Systems, vol. 31, no. 6, pp. 467 474, 2007.

[7] M. Avvenuti, P. Corsini, P. Masci, and A. Vecchio, Opportunistic computing for wireless sensor networks, in IEEE Proc. of MASS 07, pp. 1 6.

[8] A. Passarella, M. Conti, E. Borgia, and M. Kumar, Performance evaluation of service execution in opportunistic computing, in Proc. of ACM MSWIM 10, 2010, pp. 291 298.

[9] M. Conti, S. Giordano, M. May, and A. Passarella, From opportunistic networks to opportunistic computing, IEEE Communications Magazine, vol. 48, pp. 126 139, September 2010.

[10] M. Conti and M. Kumar, Opportunities in opportunistic computing, IEEE Computer, vol. 43, no. 1, pp. 42 50, 2010.

[11] W. Du and M. Atallah, Privacy-preserving cooperative statistical analysis, in Proc. of ACSAC 01, 2001, pp. 102 111.

[12] J. Vaidya and C. Clifton, Privacy preserving association rule mining in vertically partitioned data, in Proc. of ACM KDD 02, pp. 639 644.

[13] A. Amirbekyan and V. Estivill-Castro, A new efficient privacypreserving scalar product protocol, in Proc. of AusDM 07, pp. 209 214.

[14] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Proc. of EUROCRYPT 99, 1999, pp. 223 238.

[15] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications, IEEE Transactions on Parallel Distributed and Systems, to appear.

[16] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, Sage: a strong privacypreserving scheme against global eavesdropping for ehealth systems, IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 365 378, 2009.

[17] M. Li, W. Lou, and K. Ren, Data security and privacy in wireless body area networks, IEEE Wireless Communications, vol. 17, no. 1, pp. 51 58, 2010.

[18] J. Sun and Y. Fang, Cross-domain data sharing in distributed electronic health record systems, IEEE Transactions on Parallel Distributed and Systems, vol. 21, no. 6, pp. 754 764, 2010.

[19] Exercise and walking is great for the alzheimer s and dementia patient s physical and emotional health, http://free-alzheimerssupport.
com/wordpress/2010/06/exercise-and-walking/, June 2010.

[20] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, Grs: The green, reliability, and security of emerging machine to machine communications, IEEE Communications Magazine, vol. 49, no. 4, pp. 28 35, 2011.

[21] D. Boneh and M. K. Franklin, Identity-based encryption from the weil pairing, in Proc. of CRYPTO 01, 2001, pp. 213 229.

[22] X. Lin, X. Sun, P. Ho, and X. Shen, Gsis: A secure and privacy preserving protocol for vehicular communications, IEEE Transactions on Vehicular Technology, vol. 56, pp. 3442 3456, 2007.

[23] R. Lu, X. Lin, H. Zhu, , and X. Shen, An intelligent secure and privacypreserving parking scheme through vehicular communications, IEEE Transactions on Vehicular Technology, vol. 59, pp. 2772 2785, 2010.