A Secure and Privacy-preserving Framework for m-Healthcare Using Android

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
Mail id: bharatsinghal004@gmail.com, dushyant1989singh@gmail.com

Abstract

m-healthcare is as emerging services when the person at remote place need help at the time of emergency. In the application both the customers and hospital has to register to the server. After successful registration by the customer.

When customer need help While occurring of accident server is activated and finds location using longitude and latitude sent by GPS device and this location is mapped with the location of nearest hospitals. Hospital will respond to the server and send ambulance to the accident spot after getting acknowledged. An expert with android phone and a basic aid are kept in the ambulance, mobile takes snaps of the victim for every 5 seconds and sends to the hospital. With the expansion for advanced mobile phones and the propel for remote physique sensor networks (BSNs), portable social insurance (m-Healthcare), which extends those operation of social insurance supplier under An safer nature's domain to exceptional wellbeing monitoring, need pulled in respectable premium as of late.

Key Words: m-healthcare, BSN

I. Introduction

For our new system, advanced mobile telephone assets including registering control and vitality camwood be opportunistically assembled with methodology those registering escalated consideration personal wellbeing majority of the data (PHI) Throughout m-Healthcare crisis with insignificant security revelation. m-healthcare, BSN prologue m-healthcare is a standout amongst the propelled innovations 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 disease, rehabilitation. By using the advantages of wireless multimedia communication, such as current high utility, convenience, high data transmission rates, high reliability, and wide coverage, we have developed the mobile healthcare system in emergency telemedicine system, the ambulance is equipped with GSM (global system for mobile communication), GPRS (general packet radio service), 3G, or a satellite mobile communication system- technologies that facilitate the wireless transmission of videos, images, cardiographs, and pulse information of the accident victim to the emergency clinic.

This enables the physician in the clinic to assess the patients physiological condition in advance and arrange for emergency medical resources well in time, which could decrease the actual time required for treating the patient. The introduction introduces the reader to the application called mobile telemedicine. In this application both the vehicle owner and hospital has to register to the server and then the telemedicine hardware is installed in the vehicle.

Once the accident occur the telemedicine hardware will be activated and the longitude and latitude is sent to the server using GPS device. Server maps the nearest location and sends the request to all nearest hospital and wait for response. Once the hospital responds to the server ambulance is sent to the accident location and then the details of patient is sent in the form of series of images to the hospital then the doctor guides the nurse.

For our maturing society, versatile social insurance (m-Healthcare) framework need been imagined Concerning illustration a paramount requisition for pervasive registering on enhance health awareness personal satisfaction Also spare lives, the place miniaturized wearable and implantable body sensor hubs and keen phones are used on give remote social insurance following with individuals who need constant restorative states for example, diabetes and coronary illness.

Specifically, On a m-Healthcare system, therapeutic clients are no more necessary should be monitored inside home alternately healing center situations. Instead, following being provided with keen telephone and remote form sensor system (BSN) shaped toward particular figure sensor nodes, restorative clients might stroll outside Also accept the high-quality social insurance screening starting with therapeutic experts anytime and anyplace.

In this framework each bisexuality versatile therapeutic user s personage wellbeing majority of the data (PHI) for example, such that heart beat, glucose level, pulse What's more temperature Also others, could a chance to be To begin with gathered Eventually Tom's perusing BSN, et cetera sent Eventually Tom's perusing advanced mobile telephone by means of bluetooth. Finally, these majority of the data transmitted of the remote social insurance focus through 3G networks. In view of these gathered phi data, specialist and medical attendants during social insurance focal point might ceaselessly screen therapeutic users wellbeing states Furthermore too rapidly react to users life-undermining circumstances What's more spare their exists Eventually Tom's perusing dispatching rescue vehicle Furthermore medicinal work force on a crisis area in An tight auspicious plan.

Existing Framework

Previously, existing System, as stated by those sensex through the ageists of 65 is required will hit 70 million Eventually Tom's perusing 2030, Hosting multiplied since 2000. Medicinal services consumptions anticipated should Ascent on 15. 9% by 2010. Those cosset for health awareness to the nation s populace expanding What's more it gets to be An national worry Along these lines it is significant to seeing how the entrepreneurial registering standard worth of effort At assets accessible ahead different hubs could be opportunistically assembled together with provide richer functionality, they bring not acknowledged those possibility security What's more security issues existing in the entrepreneurial registering standard.

Likewise in the existing framework fittings and J2Me engineering utilized which may be really of age framework.

Proposed System

Suggested framework in our recommended skeleton plans In those security Furthermore security issues, Furthermore develops An user-centric protection entry control about entrepreneurial registering done m- social insurance crisis. The requisition we planned will be mostly utilized by any distinctive who claims a auto.

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

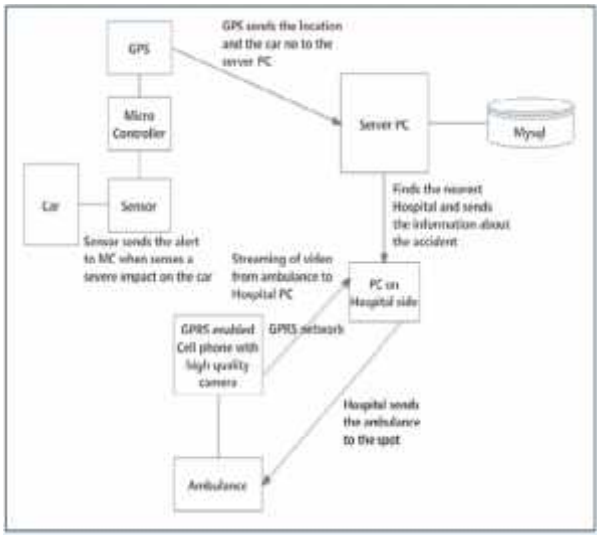


Figure 2 describe about each module and tell what exactly each module do i.e. interaction between each module and how they connect each other.

In this project all the Hospitals and the customer who owns a vehicle has to be registered. Once registration is complete a unique Hospital Number will be given to the hospital. Whenever the hospitals are activated it will send an alert message to Server Pc saying it has started functioning. Once server PC receives the Alert message it will show all the hospitals which have started functioning and will be waiting for the message from hardware.

Suppose a vehicle owner or customer, who has been registered has met with an accident, here accident is detected using metal sensors, his vehicle will be attached with the metal sensors, GPS and GSM modems. If accident is detected the GPS will retrieve the latitude and longitude of the accident place and sends message to the server which is also connected with GSM modem.

Once the Server PC receives the message, server will find place by giving the latitude and longitude values. Once we get the place, it will retrieve all the hospitals which are functioning and are within that locality and sends alert message to all those hospitals.

If any of the hospitals wishes to provide the service, it will send intimation to the server PC saying it will provide the service. Once server PC receives this message it will acknowledge the service proving and all other hospitals.

The Hospital which has taken up the initiative will send the Ambulance to the accident location. Ambulance has a mobile with camera and is GPRS Enabled and a nurse in it. Once the ambulance reaches the accident spot it

will stream the video and send it to the hospital PC. So a person sitting at the Hospital PC can monitor the video and guide the nurse who is in the ambulance.

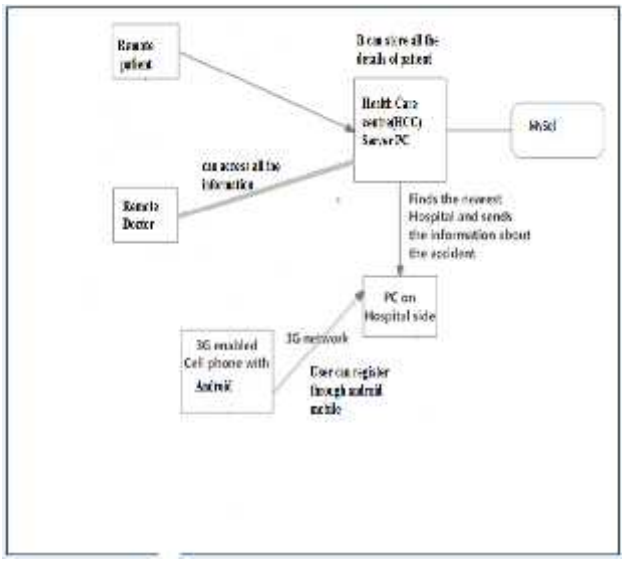
But existing system have many drawback like

- 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

Functional	Sense the human body, Send BP,HB,BT,SL to Health Care Centre, Send Ambulance details to patient, Send Complaints and opinions to HCC, Find the Report Via mobile
Non- Functional	The Automatic Alerts from HCC cannot be generated
External interface	LAN , Routers, WIFI Devices
Performance	Finding Patient Details, Patient Details efficiency fairness, The patient details are handling in secure way
Attributes	Patient body sensor details, Security, Performance, BP, HB, SL, BT, HCC, Sensors, Backbone Router, Home Healthcare Gateway



Functional Requirements

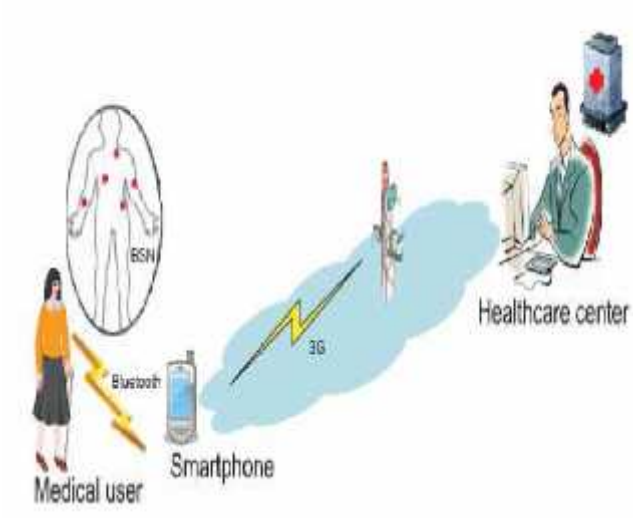
Functional Requirement defines a function of a software system and how the system must behave when presented with specific inputs or conditions. These may include calculations, data manipulation and processing and other specific functionality. In this system following are the functional requirements:-

- The Body Sensors measure the 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 cryptographic
- The Health Care Centre receives the body sensed details and decrypting the same in hospital.
- 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 Health care Gateway

Modules and their description

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

- In this module, every enrolled versatile medicinal user s individual wellbeing data (PHI) for example, such that heart beat, glucose level, pulse Also temperature Also others, could be to start with gathered Toward BSN, et cetera transmitted Toward advanced mobile telephone through Bluetooth.
- Finally, they would once more sent of the remote social insurance focus through 3G networks. In view of these gathered phi data, medicinal experts In social insurance focal point might ceaselessly watch medicinal users wellbeing states and also rapidly respond will users life-undermining particular circumstances What's more spare their exists Toward dispatching rescue vehicle Furthermore medicinal faculty with a crisis area over a firmly style.



2. Body Sensor Network

In Figure sensor system in this module, constitution region system (BAN), remote body territory system (WBAN) or muscle to sensor system (BSN) are terms used to describe the requisition of registering units. This will empower remote correspondence between a few miniaturized figure sensor units (BSU) What's more An absolute physique national unit (BCU) worn In those human body.

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

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

Input: body sensing details

Output - Sensors sensed all the patient body details and send to **HCC**

Step 1. Start *PPSPC Protocol to sense all Sensors and intermediate nodes such as back bone routers etc.*

Step 2. Choose some random numbers as patient body sensing details from patient body

Step 3. Keep all the sensing details secretly

Step 4. Then Send to the HCC

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 ICC via Hand Held Mobile Device

.Security Analysis

n this module will create a secure What's more privacy-reserving entrepreneurial registering schema to furnish elter skelter dependability of phi transform Also ansmission same time minimizing phi security evelation Previously, m-Healthcare crisis. pecifically, we i) apply entrepreneurial registering reviously, m-Healthcare crisis on attain high-reliability f phi procedure and transmission; Also ii) create user-entric security get control to minimize the phi security evelation.

.V Execution

1.Initially, first page of server

2. Login and Registration page in Android:

V.Conclusion and Future Work

The application helps a person in such a way that when he encounters an accident and there is nobody surrounding that location then there is chances of losing his life.

We have suggested a secure Also protection preserving entrepreneurial registering structure to m-Healthcare emergency, which principally exploits how to utilize entrepreneurial registering with accomplish helter skelter unwavering quality of phi procedure What's more transmission clinched alongside crisis same time minimizing those data revelation Throughout the registering. Nitty gritty security Investigation reveals to that the recommended SPOC skeleton camwood accomplish those productive user-centric protection get control.
In addition, through extensive performance evaluation. In future 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.