Development of a Mobile Remote Health Monitoring system – MRHMS

A. Abayomi-Alli
1Sound, System and Structures Laboratory
University of Pittsburgh
Pittsburgh, USA.
ada44@pitt.edu

A.J. Ikuomola
2Department of Mathematical Sciences
Ondo State University of Science and Technology
Okiti-pupa, Ondo State, Nigeria
deronikng@yahoo.com

O. A. Aliyu & O. Abayomi-Alli
Department of Computer Science
Federal University of Agriculture (FUNAAB)
Abeokuta, Ogun State, Nigeria.
yemtech40@gmail.com, abayomialliolusola@yahoo.com

ABSTRACT

In this paper the design and implementation of a mobile remote health monitoring system (MRHMS) based on wireless technologies is presented. MRHMS was able to integrate three level networks namely Body Area Network (BAN), the Personal Area Network (PAN) and the Wide Area Network (WAN). The sensors for monitoring patient’s bio-signals like blood pressure, body temperature, pulse and breathing were in the BAN. The PAN consists of the BAN as it connects the supervisor’s agent and the mobile base unit (MBU) through Bluetooth technology while the WAN was able to combine the PAN, mobile response unit (MRU) and hospital site (HS) through GPRS and Internet technology. The system is largely mobile agent based hence it is fast and responsive in real time making it ideal for proper remote health monitoring. HTTPS, SSL and TLS protocol were all employed to secure data transmission during user authentication, ensure confidentiality and data integrity. Using a GPRS based Mobile phone or PDA and the system’s mobile base unit (MBU), patients are able to send Short Message (SMS) to the paramedics or other medical staff. Real time medical attention could be given and where necessary physical consultation is done. The Doctors can view patient’s medical records remotely, recommend or prescribe drug, request for ambulance or visit patient based on data being sent from the monitoring system. After testing it was observed that MRHMS is indeed an easy, practical, inexpensive, effective and yet very secure way for communication between the healthcare providers and patients.

Keywords- Data, Mobile, Monitoring, Health, Wireless.

African Journal of Computing & ICT Reference Format:

1. INTRODUCTION

Wireless network infrastructures, notably cellular networks, are becoming a vital element for exchanging electronic data in low income countries. Several key sectors are already leveraging and the health care sector is also aiming to tackle outstanding challenges like providing basic health care services to remote communities by using cheap mobile devices [1]. In many health care facilities, however, there exists a severe need for improvement in quality of service and patient waiting times. Normally when patients want to make an appointment with the hospital staff, it becomes really tedious and time consuming. These needs must be met with an efficient and practical solution.

This solution must make use of the hospitals’ valuable resources, such as mobile health monitoring device, in the most efficient manner. Over the past, agent based systems have also been developed for the hospital service, for searching and fixing appointment over mobile phones which gives a direct reply when the appointment is made or cancelled [2].
Mobile health-monitoring devices offer great potential help for such patients who may be able to afford good healthcare without having to regularly visit their doctor. These technologies bring potential benefits to both patient and doctor; doctors can focus more on priority tasks while saving time normally spent with consulting with patients [5] and patients can move about in their environment without having to make expensive trips to the doctor – especially if they reside in remote locations [6]. The ubiquity of mobile devices in both developed and developing countries presents an opportunity to improve health outcomes through the innovative delivery of health services and information.

In the present era of information technology, the wireless body area network has emerged as a new technology for e-healthcare that allows the data of a patient’s vital body parameters and movements to be collected by small wearable or implantable sensors and communicated using short-range wired or wireless communication techniques. This has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems. Through the health monitoring system real-time and continuous triage information can be distributed to health care providers. Light weight and no-intrusive biomedical sensors like pulse oximeter and electrocardiogram are easily deployed for continuously monitoring of the vital signs of a patient and deliver the data to the first responders [7] [8].

Mobile healthcare (m-healthcare) systems are regarded as a solution to healthcare costs without reducing the quality of patient care [9]. Common architectures for health monitoring system involve; Wireless sensor networks (WSNs) and smart phone technology has opened up new opportunities in health monitoring system. The integration of the existing specialized medical technologies with cell phone and wireless sensor networks is a very promising application in home monitoring, medical care, emergency care and disaster response. However, the accessibility and privacy protection of the data collected from a body area network (BAN), personal area network (PAN) and wide area network (WAN); to and from the client and healthcare provider while stored inside BAN Data Repository within a required time is a major challenge. These data transmitted to and fro require high demand for immediate access with security and practicality. The security and privacy protection of data collected through the Bluetooth enabled mobile health monitoring system connected to the patient that is being transmitted by the mobile base unit to the server is another major challenge.

2. REVIEW OF RELATED WORKS

[10] Developed an episode-based patient care cycle with eight stages. The eight stages of doctor–patient interaction in the context of the current episode-based care where the interaction between the patient and doctor happens only during patient visits. This approach gives doctor- patient complete interaction and it warrants a sporadic contact for easy treatment. However, it is time consuming for the doctor to attend to the patient and the patient would have to be hospitalized. In case of seriously ill patients, all beds in hospital will be occupied and therefore many emergency cases may be deprived the required attention. The patient could die of complications between these sporadic contacts and the doctor would not even know. Finally the security of patient’s data is a major challenge due to physical assessment.

[11] Proposed an agent-based mobile e-health monitoring approach. A multi-agent architecture for mobile health monitoring was presented involving a team of intelligent agents that collate patient data, reason collectively and recommend actions to patients and medical staff in a mobile. The study also presented a generic agent-based e-Health monitoring framework that is used to assist in the doctor-to-patient interaction spanning multiple remote locations and hospitals. The approach delivered better healthcare to patients, especially in the case of home-based care of chronic illnesses, the cost of which is increasing because of the ageing population in the world. The security of mobile agents is a major challenge to the design. Another drawback is possibility for Internet dysfunction altogether since it relies on the Internet as its data and information carrier.

[12] Proposed a multi-agent system for pervasive healthcare. It aimed at the development of an effective and efficient solution for pervasive healthcare by adopting the concept of pervasive informatics and using the methods of organizational semiotics. The framework improved the healthcare quality by timely and reliable detection of anomalies and enhances the efficiency of the healthcare professionals by providing appropriate medical attentions when needed. The security of patient’s data was not adequately dealt with and the mode of data storage has little constraint in terms of hospital activities.

[13] Developed MediNet for staying connected in a mobile healthcare system. The main aim of the design was provide continuous high level service to patient in the face of communication problems leading to improved acceptability and trust of the system. The security of patient’s data is also a major challenge as there many connections within the system therefore creating loops for security breaches.

[9] Developed mobile healthcare system using near field communication technology. The authors developed a system to facilitate the provision of healthcare to people anywhere, anytime using mobile devices that are connected through wireless communication technologies. This system makes the entire process of patient record keeping easier, more accurate and comprehensive and more efficient. Data security for the patience is a major challenge and the system is prone to interference.
3. DESIGN AND METHODOLOGY

This section discusses the design consideration of the Mobile Remote Health Monitoring System (MRHMS). The architecture of S-RHMS is presented in Figure 1.

3.1 Design Considerations

In this design, the following are incorporated into mobile health monitoring system.

Figure 1: Architecture of the Mobile Application for Remote Health Monitoring System.
Security of data – prevention of threats or unauthorized disclosure, modification and withholding of information.

Improved efficiency – effective and improved mobile health monitoring system by intelligently handling patient readings and surveys the patient’s environment, allowing experts to visualize the current condition of the patient and informing response personnel such as paramedics to respond to a situation.

3.2 Architecture of MRHMS
See Figure 1 for the architecture of S-RHMS. The SS-MHMS comprises of three levels network namely: the Body Area Network (BAN), the Personal Area Network (PAN) and the Wide Area Network (WAN).

Body Area Network (BAN) – In the BAN system, sensors are attached to patient’s body area in order to capture bio-signals, including blood pressure, body temperature, pulse and breathing. It is mainly divided into three parts i.e. the Patient, the digital device and front end.

Figures 2: Body Area Network
Figure 2 above describes the main components of the Body Area Network system and the interactions between its components. The following are the different components defined in the body area network:

- **Patient:** A device, such as a photoelectric cell, that receives and responds to a signal or stimulus. The sensors collect necessary readings from patient’s body and sends to the front-end node in form of low frequency electromagnetic waves.
- **Sensor:** A device responsible for actuating a mechanical device, like one connected to a computer by a sensor link.
- **Actuator:** Hub for all the sensors and actuators in the BAN. It records all the data from all the sensors and actuators, and can send them to the MBU.

The BAN is a set of different sensors and actuator connected to body of the patient that receive all the patient data and then records them in the front end. These data are further forwarded via the Bluetooth to the mobile base unit (MBU) in the Personal Area Network-PAN

Personal Area Network – The personal area network includes the BAN and the Supervisor Agent with the Mobile Base Unit. The BAN and its components functionality have been explained. When the BAN communicates the supervisor agent and mobile base unit through Bluetooth; the whole network becomes a Personal Area Network (PAN).

Figures 3: Personal Area Network
The PAN component is GPRS based connects the BAN to users who communicate through the internet. If the agent is to forward the patient’s data to the hospital servers, the supervisor agent will commence the transfer via GPRS or 3G technology. To transfer data, the supervisor agent begins to encode data into a format which the manager agent of the server understands. The PAN consists of the following components:

- **Body Area Network (BAN):** The sensors collect necessary readings from patient’s body and sends to the central node in form of low frequency electromagnetic waves.
- **Supervisor Agent:** The Supervisor Agent operates between the mobile device and the hospital system, controlling the entire back-end. Firstly, it receives real-time medical data from a patient including the blood pressure (systolic/diastolic), body temperature, breathing and pulse. It saves the data into a repository, and then uses a specific pattern recognition module to analyze the data and compare it with normal conditions. If the value of data exceeds normal range (threshold), the agent sends an emergency alert message to a doctor or any other person with authority in the hospital via the manager agent, to take appropriate emergency measures. And if the value falls within normal range (threshold), services will be discontinued when data is saved in the repository.
- **Mobile Base Unit (MBU):** This is a mobile device or smartphone that is GPRS based e.g PDA or Mobile Phone. It enables the transfer of data to the back end via the internet as at when required.

Wide Area Network (WAN) – This is made up of the PAN, Hospital Site and the Response Team. The WAN provides connectivity between the patient and remote health care personnel who might be geographically far apart. Though, the operation of web application servers running at hospital sites, the server (manager agent) is program to collaborate with the supervisor agent. Figure 4 shows the components of the WAN.
Hospital Site (HS) – The second part of WAN is the HS which receives information from the PAN. This is made up of the Back-End and End-user application.

Back-End System (BESys): The back-end system composed of a wireless service broker (WSB), a Surrogate Host (SH) and a BANData Repository. The BESys are installed in some of the GPRS service providers, as well as in some of the hospital or health care centers.

- **Wireless Service Broker (WSB):** authenticates and authorizes the MBUs. The WSB has a gate agent. The gate agent verifies a patient’s authentication of his request for services. Patients have different access rights to the system, in accordance with various privileges given by their roles.

- **Surrogate Host (SH):** this is the main server where wireless sensor and actuator objects are surrogated inside the wired internet and where medical data is received. The SH has a manager agent.

- **Manager agent:** This agent determines whether a patient is in a critical condition based on medical data transferred from the BAN system. If it is determined there is an emergency, the data is transferred to the hospital system for enacting emergency measures immediately after being stored in the BAN Data repository. The agent also searches for the doctor in charge and related hospital support staff. This agent sends a message including the patient’s historical data and diagnosis to the doctor in charge.

  In case it is not an emergency, the data is merely stored in the BANData repository. For data stored in BANData repository, necessary data is regularly saved to the central database (EUA) of the hospital. These real time data will be deleted after certain period unless there is an emergency.

- **BANData Repository (BDR):** This acts as a client to surrogate host and also writes the medical data (i.e. measurement to persistent storage).

End-User Application (EUA) – The end-user application is a computer system in the hospital which is used to access the information from the sensors and actuators and to send new configuration parameters to the BAN through the access to the Back-end system. This is either a server in the hospital that access the data from the surrogate host or BANData Repository and stores it in the existing patient’s hospital data base or user computer of the authorized employees that access the information from the BANData Repository from inside and outside the hospital.

Mobile Response Team – This is a team of medical professionals e.g. nurse, paramedic, doctors, etc.

The response team (i.e. nurse, paramedic, doctor etc.) on duty logs in to the system to view the patient’s monitored progress in real time, whenever they received a message or alert from the manager agent. The doctor’s diagnosis of a patient is aided by message from the manager agent. As well as this diagnosis, if the patient needs attention, the Response Agent (RA) sends an opinion of the doctor to the patient through the Back-end system.

3.3 Security

In general, security means preserving and protecting property or interests from intrusions. The main principle used to achieve this is to restrict access to the specified resources, and allow access only to trusted parties that are able to prove their identity. Given this definition, security is based on these main issues.

- **Authentication:** This is to ensure that the provided credentials from the user are in order,

- **Confidentiality:** This is the prevention of any unauthorized disclosure of information,

- **Integrity:** This is the prevention of unauthorized modification of information,

- **Availability:** This has to with the prevention of unauthorized and unwanted withholding of information or resources.
Authentication – As a prerequisite for enabling access to any system that contains private information it is required that the user is identified and authenticated. Through identification the user announces who he/she is, and through authentication the user proves who he/she claims to be. In order to perform user identification, some type of unique user identifier, such as a username or user ID number, is required. When it comes to performing a user authentication process some of the traditional approaches used are:

- something a user knows (the user has to know some “secret”, e.g. password or PIN number), something a user holds (the user has to have a physical token, e.g. One-Time Password (OTP) generator or identification card)

Key and Password Management – As long as HTTPS is used to protect data transmission, only a valid certificate recognized by the mobile device is needed. Rest of the key management is taken care of by the SSL/TLS protocol on which HTTPS is based. When passwords are used for user authentication, some distribution and recovery mechanism should be in place to guarantee availability of the service and the data, in case passwords are lost or forgotten. As long as the credentials are the same on both the client and on the server, and they are not stored on the client, it is quite easy to change centrally only on the server, although it might be challenging to distribute them securely to the collectors in the field.

Confidentiality – The first thing we checked was whether data was properly protected from unauthorized disclosure both when stored on the mobile device and when transferred to the server (SH). In particular we verified that proper encryption was in place.

Communication – All MDCS we investigated use or support HTTPS to protect the transmission of data between the client and the server. In general this solution is more than adequate to ensure that data in transit between client and server is protected, under the right conditions. That is, as long HTTPS is used with certificates signed by a trusted Certificate Authority (pre-installed on the mobile device by the developer), and the protocol on which it is based, is correct.

4. IMPLEMENTATION

In this section the MRHMS design is implemented based on the following software and the hardware requirements.

4.1 Choice of Software Tools
Java was chosen as the application programming language for the development of the GUI and the front-end applications. Similarly, MySQL/PHP was chosen as the choice language for our back-end applications based on the following reasons:
- Java is an open source language
- MySQL and PHP are also open source languages.
- the Flash Builder
- Notepad ++
- Macromedia Dreamweaver
- the languages offer a rapid design development and deployment support for creating and consuming web services.
- the provide important features of form designers and visual controls for creating rich-Windows-based applications in form of GUIs.

4.2 Choice of Hardware Tools
This project works fully with the following hardware component:
- A PDA- Personal Digital Assistant to transfer readings to the Mobile Base Unit through Smartphone
- A Smartphone of running Android 4.2 or higher
- A server (Surrogate Host) which bought online.

4.3 Interfaces of the Patient Application
Whenever the patient fills the form and submits, the data is sent and stored automatically in the BAN DATA repository. This makes the patient a registered and legitimate patient in the hospital. The registration PIN- Personal Identification Number will be supplied by the Hospital Management to the applicant as part of the security to login when next it is required. The password is a particular code from the applicant which must be taken care of and strictly noted by the user. Any necessary information to be added to this form can be determined by the hospital management.

Figure 6: Patient’s Registration Interface

Input Interface for the Patient’s Data – It takes the body temperature, the blood pressure, the heartbeat rate and the respiratory readings to be sent to the Mobile Base Unit within the front end. These readings are to be routed to Ban Data Repository at the Back end. Figure 7 shows the patients login page.
The output data sent is displayed by Figure 8 and must have been recorded in the Server. In case any of these readings goes beyond the threshold, the manager agent in the back end works on them and determine what next to do.

The registration PIN- Personal Identification Number is supplied by the Hospital Management to the user as part of the security to login when next it is required. Any other information to be supplied will depend on the hospital’s request to scrutinize the applicant.

The doctor’s activities form is shown on Figure 10 while the database output is displayed on Figure 11.

**1.4 Interfaces of The Doctor Application**

The doctor’s registration form is displayed in the Figure 9. It allows any interested but qualified physician to submit the required information. This information goes to the repository. An acknowledgement is returned to the applicant authenticating the user.
5. CONCLUSION

This study has presented architecture for monitoring of human health conditions based on emerging wireless mobile technologies. It also provides the basis for the use of intelligent agents to deliver better healthcare to patients, especially in the case of remote or home-based treatment. It also takes care of every interested individual whose monitoring of his or her health is paramount. The application of this project work can be applied to many e-Health services with the home doctor-to-patient monitoring from a remote location and in any part of the world for illnesses and responding to emergency situations as at when necessary. The Bluetooth enabled bodily attached device that will take readings from the patient is highly scarce and very costly. As the telecommunication infrastructure is fast growing, we should see enhanced communication quality and faster transmission of data such that quality video and voice content can be captured by agents to allow healthcare professionals to provide better patient services with the data online and made available for any qualified registered physician.

REFERENCES


