International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321 - 8169
Volume: 3 Issue: 2 792 - 795

A Survey of Research on Health Monitoring System using Mobile Cloud Computing by Home Node Base Station

Sandhya Rani U
Assistant Professor & HOD, Department of CSE
Sai Vidya Institute of Technology,
Bangalore, india
e-mail: sandhyakalmady@gmail.com

Prasanna Kumar S B
Student (M-Tech 4th sem), Department of CSE
Sai Vidya Institute of Technology,
Bangalore, india
e-mail: puliprasanna.s.b@gmailcom

***Abstract*—**This paper presents a E-health monitoring scheme based on HNB (home node base station) and mobile cloud computing. In this method, the health data of each user is captured by using sensors and sent to the corresponding devices (i.e desktop, laptop, mobile). From that device the health data is transferred to cloud under which the mobile device is registered. In HNB it is verified whether the user's health is normal using a database stored inside the HNB. If any abnormality is detected it will shows some indication through some sounds or light. The E-health data are send to cloud for each 15 seconds. In cloud also the data is verified with the normal data and if any abnormalities found it will indicate by sending message to the corresponding healthcare center. The health data in the cloud are stored with high security and only authentic healthcare center can access the data. Based on health data the healthcare centre takes proper action to cure the patient.

Keywords- *Mobile cloud computing, Home node base station, E-health monitoring, Healthcare centre, E-health Data*

*****

I. INTRODUCTION

E-healthcare system or services are gaining popularity day by day. The healthcare systems or services that are supported by electronic processes and communication are known as e-health care systems [1]. Telemedicine and mobile health (m-health) are the essential form of e-health by which a person can aware of his or her physical and psychological fitness at a distance [2-4]. E-healthcare applications require a wireless body sensor network (BSN) to support multiple data rates with reliable and energy efficient data transmission. Wireless BSN provides a secure, efficient and reliable platform for e-health monitoring service over the traditional health monitoring services [1]. Mobile Cloud Computing (MCC)[5-6] takes an important role for mobile health (m-health) application in respect to the limitations like quality of service, physical storage, security, privacy, first response, medical error due to which the traditional healthcare system suffers. A real time health monitoring system has been described in [3] where a sensor is attached with the existing medical equipment's that are inter-connected to exchange service with the help of cloud environment.

To support e-health monitoring, a pervasive environment is implemented in using which data accessing, emergency management system, networking problems for heterogeneous network are solved. But still some major issues for quality of service like low bandwidth, latency, security, privacy, and context awareness are not resolved. HNB which is also known as Home Node Base Station (HNB) is a low power base station with the help of which the solutions to these problems can be determined.

II. HOME NODE BASE STATION

A. Body Sensor network

Wearable health monitoring systems based on wireless body sensor networks (BSNs) offer many advantages over conventional health monitoring approaches. First, cabless to the human body; thus, monitoring distance can be greatly increased. Second, a large number of sensors can be placed on patients if needed for real-time biomedical monitoring in either stationary or mobile scenarios. However, there is a significant gap in the current research activities on BSNs to meet the requirements of medical monitoring applications. In general, medical monitoring requires multiple data transmission rates, very high communication reliability, and relatively low transmission power. Traditional wireless in network aggregations that fuse data from multiple end nodes may not be applicable in medical monitoring applications. The development of on body information processing aims to reduce the total amount of data to be transmitted and increase transmission quality, which is demanded by BSN-based telemedicine applications. In error-prone wireless channels data loss in transmission is commonplace. However, most medical applications have a very strict requirement on lossless transmission of medical data. Any loss of important information in medical applications may lead to severe medical accidents and subsequent litigation issues. In order to ensure transmission quality for medical signals under limited power and computational resources, it is desirable to allocate resources unequally to protect more important information conveyed through wireless BSNs.

In this article we proposed a secure BSN architecture enabling real time and effective healthcare monitoring, especially for secure wireless electrocardiogram (ECG) data streaming and monitoring. A cross layer framework is developed based on unequal resource allocation to support biomedical data monitoring applications.

In this scheme important information (e.g., major ECG data) is identified, and extra securities are taken to protect its transmission. In this article we integrate biomedical information processing and transmission in one framework, where data transmission in a BSN proceeds with secure, energy efficiency and minimum delay. Energy efficiency refers to savings in total energy consumption of medical sensors, health nodes, and data terminals without degrading system performance. It is achieved through the energy-constrained signal quality maximization described later. In

particular, we present a wearable ECG sensing system consisting of small and low-powered health node sensors for wireless ECG monitoring.

The rest of the article is outlined as follows. The next section reviews related work in the literature and highlights the contributions of this work. We then introduce the sensor nodes we developed for real-time ECG streaming and monitoring. We propose a BSN architecture that can meet the requirements for real-time health monitoring applications. We then present a secure resource-aware optimization scheme to achieve energy efficiency, reliable signal transmission, and information privacy. We evaluate the performance of the proposed architecture through both experiments and simulations. These results are compared with those of existing techniques, followed by the conclusions presented in the final section.

B. General packet radio service

GPRS is a type of wireless data connection. It stands for General Packet Radio Service. Wireless data service that extends GSM data capabilities for Internet access, multimedia messaging services, and early mobile Internet applications via the wireless application protocol (WAP), as well as other wireless data services. GPRS is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications. GPRS usage is typically charged based on volume of data transferred, contrasting with circuit switched data, which is usually billed per minute of connection time and data size used. Usage above the bundle cap is either charged per megabyte or disallowed.

GPRS is a best effort service, implying variable throughput and latency that depend on the number of other users sharing the service concurrently, as opposed to circuit switching, where a certain quality of service (QoS) is guaranteed during the connection. In 2G systems, GPRS provides data rates of 56–114 kbit/second. 2G cellular technology combined with GPRS is sometimes described as 2.5G, that is, a technology between the second (2G) and third (3G) generations of mobile telephony.

III. MOBILE CLOUD COMPUTING

Mobile cloud computing is defined as extension of cloud computing with a new ad-hoc infrastructure based on a mobile device [4]. In scenario of mobile cloud computing there are two viewpoints. One is a simple viewpoint and other is mobile device viewpoint. Simple viewpoint refers that both data storage and data processing is carried outside the mobile devices. Cloud resources are utilized for processing and storage purpose. The advantage of this concept is that mobile cloud computing applications are not constrained to a certain kind of mobile devices or operation systems. Also no need to worry for the storage capacity and computation speed limitations. Mobile Cloud Computing services are implemented in mobile wireless environment, incorporating several challenges such as the dependency on continuous network connections. Also Mobile Cloud Computing concepts depends always-on connectivity and will need to provide a scalable and high quality mobile access.

A. Network delay and limited bandwidth in the mobile network

First, Mobile Cloud Computing may face the challenge from the transmission channel due to the intrinsic nature and constraints of wireless networks and devices. This is especially true when it comes to high bandwidth internet and immersive mobile applications, e.g. online gaming and augmented reality that require high-processing capacity and minimum network delay. These will most probably continue to be processed locally on higher end smart phones and mobile tablets. Mobile broadband networks generally require more execution times for a given application to run in the cloud and network delay issues may deem certain applications and services unfit for the mobile cloud.

B. Various access scheme in mobile environment

Mobile Cloud Computing would be deployed in a heterogeneous access scenario with different radio access technologies such as GPRS, 3G, WLAN, WiMax. Mobile Cloud Computing requires wireless connectivity with the following features:

- Mobile Cloud Computing requires an “always-on” connectivity for a low data rate cloud control signalling channel.
- Mobile Cloud Computing requires an “on-demand” available wireless connectivity with a scalable link bandwidth.
- Mobile Cloud Computing requires a network selection and use that takes energy-efficiency and costs into account.

C. Elastic application models

Cloud Computing services are scalable, via dynamic provisioning of resources on a fine-grained, self-service basis near real-time, without users’ consideration for peal loads. This requirement is particularly important towards mobile cloud computing scenario. Mobile applications can be launched on the device or cloud, and can be migrated between them according to dynamic changes of the computing context or user preferences. Also, limited resource of mobile device will restrict application processing. Thus, elastic application model should be proposed to solve fundamental processing problem

D. Security and privacy

Cloud computing users prove their identities with digital credentials, typically passwords and digital certificates. If an attacker could fake or steal these credentials, the cloud computing system will suffer from spoofing attacks. In mobile cloud computing the problem is even severe because mobile devices often lack of computing power to execute sophisticated security algorithms. Moreover, it is difficult to enforce a standardized credential protection mechanism due to the variety of mobile devices [4].

IV. PROPOSED SYSTEM

A *Working Principle of Proposed Scheme*

HNB and MCC based proposed m-health monitoring scheme requires the following components:

- Body sensor network
- Cloud
- HNB
- Internet connectivity

The working model of proposed E-health scheme is pictorially depicted in Fig.1. HNB and cloud are connected via internet connectivity. To provide proper security between HNB and Cloud over the internet a security gateway is maintained.
The working principle is given below:-

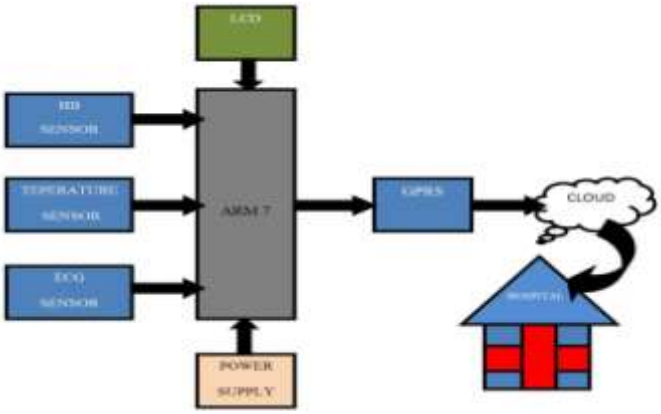

FIG 1: The proposed E-health care system

Health data capturing by BSN and transmission to HNB, the BSN captures the physiological information (body temperature, blood sugar level, blood pressure, respiration rate, ECG etc) of the mobile user and sends it to the corresponding HNB. Health data checking at HNB, HNB compares the received health data against the threshold values of the respective health parameters stored in a database which is stored inside the HNB, this phase is described in subsection B. Health data transmission from HNB to cloud, for every 15 seconds the health data captured is sent to cloud, this phase is described in section C. Data stored in cloud for access by health Centre, After the health data are received, stored in cloud with the location information, so that health centre can access the data and take necessary action like sending advice to the patient via a voice call/SMS or sending ambulance to the patient location to take care of his or her.

B *Verification of User Health at HNB*

In HNB a database is maintained which stores the range of values for the health parameters of a normal and healthy person. If the health data values obtained from the Sensors do not fall in the range stored in the database it indicates abnormal health condition. Then the health data are sent to the cloud.

C *Security in Proposed Scheme*

The HNB is connected to the cloud through a security gateway. As the user health data are transmitted from
the HNB to the cloud via the security gateway, secure data transmission is achieved. On the other hand to provide health data security in cloud, a user id and password are generated when for the first time the data are received from the user. The generated user id and password are sent to the user so that the user can access the data on cloud. To achieve high security a two-way verification is also introduced. When the user gives the corresponding user id and password to access the data, a verification code is sent to the mobile phone of the user. After giving the correct verification code, the user can access his or her data on cloud. The id of the health care centre which first accesses the data of the patient is attached to patient information stored in the cloud and phone number of the health care centre is sent to the mobile phone of the corresponding patient. For each health care centre a user id and password are maintained, so that no one except that particular health centre can access or see the data. As except the intended health care centre and the user no one can access the data, privacy, authentication and integrity are guaranteed from the view point of user and health centre both. If the data of a patient is not updated in the cloud for more than one year, the data values are erased from the health database maintained in cloud.

CONCLUSIONS

In this paper we have proposed HNB and mobile cloud computing based a mobile health monitoring scheme. The physiological condition of the user is captured using body sensor network. The health data are sent to the HBN by some communication media (wired or wireless). HBN checks the data and if any abnormality (i.e variation in health condition) is detected it will glow some indication light, the data are sent to the cloud where user id and password are generated and sent to the respective user. The id of the health care centre that first tries to access the data is attached to the corresponding patient data in the cloud. For each health care centre a user id and password are maintained, so that no one except that particular health centre can access or see the data. The health care centre takes necessary action either by giving advice through a phone call or sending message or by sending ambulance to the victim based on the health condition. Thus health care service is provided to the patient as consumer where both the provider and corresponding consumer have access to the health data with the help of the user id and password and users can easily interact with their health care providers using the proposed scheme. Data transmission from HNB to the server occurs through a security gateway. Hence during transmission authentication, privacy and integrity of the patient data are achieved. User id and password are maintained so that only the respective user and the corresponding health care centre can access the data in the cloud and thus patient data security is achieved in the cloud.

ACKNOWLEDGMENT

I would like to extend my sincere gratitude to Sai Vidya Institute of technology.

REFERENCES

[1] H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynezhad, "Resource Aware Secure ECG Healthcare Monitoring Through Body Sensor Networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 12-19, 2010.

[2] S. E. Kern and D. Jaron, "Healthcare Technology, Economics and Policy: An Evolving Balance," IEEE Engineering in Medicine Biology Magazine, vol. 22, no. 1, pp. 16–19, 2003.

[3] J. Zhang, J. N. Stahl, H. K. Huang, X. Zhou, S. L. Lou, and K. S. Song, "Real-Time Tele consultation with High-Resolution and Large- Volume Medical Images for Collaborative Healthcare," IEEE Transactions on Information Technology Biomedicine, vol. 4, no.2, pp. 178–185, 2000.

[4] R.G. Lee, H.S. Shen, C.C. Lin, K.C. Chang, and J.H. Chen, "Home Telecare System using Cable Television Plants—An Experimental Field Trial," IEEE Transactions on Information Technology Biomedicine, vol. 4, no.1, pp. 37–44, 2000.

[5] S. S. Qureshi, T. Ahmad, K. Rafique, and S. U. Islam, "Mobile Cloud Computing As Future For Mobile Applications Implementation Methods And Challenging Issues," IEEE CCIS, 2011, pp. 467-471.

[6] L. Guan, X. Ke, M. Song, and J. Song, "A Survey of Research on Mobile Cloud Computing," IEEE/ACIS, 2011, pp. 387-392.