Smart and Secure Future Health Prediction Using Hadoop

Dr.Shubhangi D.C
HOD Dept. Of CS & Engg, VTU PG Center,Kalaburagi, Karnataka ,India.

Aafiya Noorian
PG Student Dept. of CS & Engg,VTU PG Center, Kalaburagi, Karnataka, India.

Abstract – In today's modern world Internet of things has become prominent due to advances in information and communication systems that has eventually led to the growth of this new technology. IoT is a technology of inter-networking computing devices that can transfer the data over the network. In the field of healthcare, IoT has number of applications such as remote monitoring of patients through sensors, smart sensors. It helps physicians to deliver care to patients in areas such as healthcare management system, real time monitoring and patient information monitoring. Body Sensor Networks (BSN) is a wireless technology of wearable devices that are computing devices that helps to monitor patient using lightweight, low-powered sensor nodes. This new technology faces security issues as the patients sensitive data will be transferred through different channels making it vulnerable. On the daily basis healthcare management system generates large volume of data probably BIG DATA that may contain structured, semi-structured or unstructured data that can be further analysed. In this paper, we design a probabilistic data collection mechanism and on the collected data we perform a correspondence analysis. Finally we design a statistical prediction model to anticipate the future health condition of the most patients in accordance with their current health status.

Index Terms – Internet of Things(IoT), Body Sensor Network(BSN), Health Care System, Hadoop, Future Health Prediction.

1. INTRODUCTION

In the past few years there is a rapid increase in population of elder aged group people and also we found that they suffer from at least one chronic disease that causes them difficulty in taking care of their health. So the modern health care management system ensures to provide care and good quality of life to the elder people using a prominent technology known as Internet of Things (IoT). IoT has become more value and productive now a days. IoT involves Body Sensor Networks (BSN) that are wireless wearable sensors that are implanted on patients body that collect patient sensitive information and helps to ensure security of collected information so that it is not hostile. The sensors used may be body temperature sensor, blood pressure sensor, heart beat sensor and motion sensor. These sensors seamlessly interact through secure channels. The data collected by Healthcare management system is huge that has large volume that may be structured, unstructured or semi structured. The massive data is termed as BIG DATA This data has all 5 characteristics of BIG DATA that is Volume, variety, velocity, value, veracity .The collected patient data are in petabyte or in zeta byte, which describe the volume. The velocity is the speed at which the data is received from the patient. The type of data such as structured, unstructured or semi-structured is expressed in terms of Variety. There has been a recent development in mobile devices which can be paired with sensors so that the data can be collected .Therefore a massive amount of patient data is generated in a healthcare system that is stored and requires analysis to be performed on it. Therefore a distributed storage and processing environment of cloud is required to store and processing environment of cloud is required to store, process and finally analyze the data that is accessible irrespective of time and place.

2. RELATED WORK

In [1] presented the complete initial design of CodeBlue and prototypes of several components. The finger pulse oximetry node has been completed and development of an ECG node is currently in progress. Based on tinyOS Surge protocol an adaptive spanning-tree multi-hop routing algorithm was explored and to reduce interference, dynamic transmission power scaling was incorporated. A lightweight public key infrastructure based on elliptic curve cryptography is currently being tested. A sophisticated programming model using abstract regions for routing, data sharing, and aggregation has also been developed. The advanatges are It joined dynamic transmission control scaling to limit obstruction and It is low-control gadget**.**The Disadvantage are Communication challenges: The principal test is secure, dependable, adhoc communication among gatherings of sensors and versatile, handheld gadgets.Computational challenges: Sensor hubs have extremely constrained computational power, and customary security and encryption procedures are not appropriate to this domain.

In [2] presented the huge opportunity in the 'point-of-care' access and recording and transmission regarding patient information will continue to propel the healthcare industry so

as to approach increased mobility. The importance here is to transpose recognition that mobility in healthcare settings increasingly refers to – the healthcare providers (health 'outsourcing), the mobility of sensor/actuator devices, and of the patient (users) themselves. MobiCare is an ongoing project of which much work remains to be done and it influences the point-of-care patient access using which benefits like healthcare quality, a programmable service architecture flexible service composition and a full-scale medical system integration are provided. Apart from the proof-of-concept prototype, the process of scrutinizing other long-term, challenging research problems in MobiCare that includes the network security of body sensors, sensor code updates and upgrades in terms of reliability and security, the prospective legitimate obstructions involved and the privacy issues that arise with updating remote codes dynamically. The Advantages are It enhances nature of health care, a programmable administration engineering, adaptable composition of service. The Disadvantage is that It is not reliable and secure.

In [3] presented the first experimental evaluation of prominent device pairing methods. Results show that some simple methods (e.g., comparison of image and visual number) that are secure, fast and readily acceptable by users. Devices that have proper –quality displays are drawn to settings.HAPADEP variant is desirable for more constrained devices that require very little user interference that is fast, without any error. For devices that do not have screens, speakers and microphones .LEDButton or Vibrate-Button are most suitable.The Advantage is It is quick and secure as well as acceptable by users.The Disadvantage is User evaluation for each method is not yet done.

In [4] realized a patient monitoring system based on wireless body-worn medical sensors. An instinctive way was carried out in which the set-up protocol designed enables fast association of multiple medical sensors to individual patients.For reliability and safety of overall system the integrated patient and clinician identification was considered. Presently, each network node is pre-configured with a unique address.The main focus of our paper is on analysis of future health prediction by designing a stochastic model with respect to current health status of patient.The Advantage is It is safe and reliable.The Disadvantage is Dynamic allocation of device addresses is not yet done.

Summary of Related work is depicted in Table 1

First author	Description of technology designed	Strengths of technology	Limitations of technology
David Malan	CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care	Incorporated dynamic Transmission power.Scaling to minimize Interference. Low power device	Security, Realibility. Sensor nodes have less computational power.
Rajiv chakravorty	A Programmable Service Architecture for Mobile Medical Care	It improves quality of healthcare, a programmable service architecture, flexible service composition	It is not reliable and secure.
Arun Kumar	Caveat Emptor: A Comparative Study of Secure Device Pairing Methods	It is fast and secure as well as acceptable by users.	User evaluation for each method is not yet done.
H.Baldus	Reliable Set-Up of Medical Body-Sensor Networks	It is safe and reliable.	Dynamic allocation of device addresses is not yet done.

Table 1. Summary of Related work

3. PROPOSED MODELLING

In our proposed solution our main focus is on security of patient data that is collected through Body Sensor Networks in today's modern health care system. In most systems Security is defined at the system level. The sensor nodes in healthcare are wireless that are used for the purpose of communication which lead to various security threats to these systems. Cloud encounters some security problems from wireless sensor devices. The data collected by sensor nodes is stored in HDFS and the high performance of cloud platform provides a framework called Map Reduce that is scalable and distributed parallel processing framework, used mainly for data processing. A massive amount of data on cloud can be processed in parallel by Map Reduce framework. The important benefits of using Map Reduce framework are the scalability and fault-tolerance during processing of huge amount of data on a large cloud. The modern healthcare system using BSN, also known as BSN care can assure systematically achieving those requirements. Security is one of the most important aspects of any system. People have different views about security and hence it is

described in different ways. Our proposed system starts with developed model which collects the data from the sensors and sends the data to a Local Processing Unit, which then sends data to the server. This model also provides mutual authentication, anonymity, secure localization, defeat forgery attack and reduce computation overhead using Lightweight Anonymous Authentication Protocol and Data Privacy and Data Integrity using AES Encryption. The advantages of our proposed Architecture are BSN-Care can efficiently establish various security requirements of the BSN based healthcare system and It is highly imperative that the system should poses all the aforesaid security requirements and eventually can resist various security threats and attacks like modification of data, imitation, intrusion, replaying etc.

The proposed architecture for this system is given below. It shows the way this system is designed and brief working of the system.

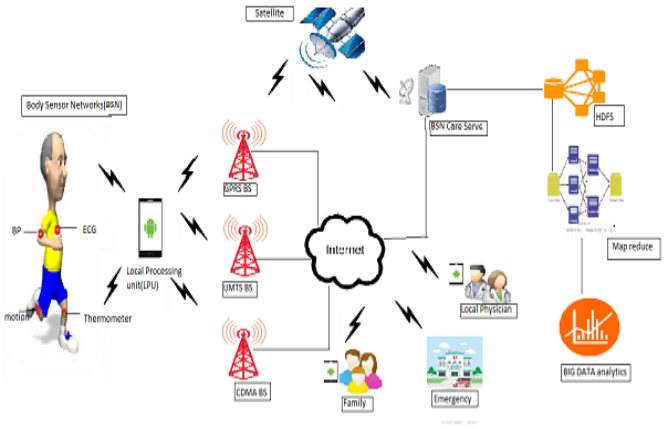

Figure 1. System architecture

Figure 1. shows the system architecture in which the data is collected from the person wearing implantable sensors that may be heart beat sensor, blood pressure sensor(BP),body temperature sensor and motion sensor,the sensor data is forwarded to the LPU or a coordinator (smart phone) and if there are any abnormalities detected with the person, the LPU communicates with the server through internet by sending an alert to either family member, local physician or an emergency care unit. Our proposed system has following modules:

A. Module 1: Data Collection Module

This is the first module of our system.In this module the the current body status of patient and details are forwarded to the LPU (in our case a smart phone is used as LPU) by sensors that are connected to our body and collect appropriate data. The sensors used in this project are blood pressure sensor, Heartbeat sensor, motion sensor and temperature sensor. The sensors are connected to an arduino board and the details of the data collected by the LPU are transferred using Bluetooth.

B.Module 2 :Lightweight Authentication Module

In this module the User of the body sensor network should register in the smart phone using the Android app ,while registering user enters the relevant personal information such as user ID ,password, name, email id, mobile number of family member, doctor details all these details are forwarded to the server and the details are stored in the database. After this process user should authenticate the phone. To authenticate the phone user uses the IMEI number as the phone ID which is unique code for a particular handset and send this ID to the server and it services details of the LPU in the database .On receiving the request from the LPU, Shadow keys, emergency keys are generated and other parameters using the Light weight network authentication algorithm and the details are saved in the server and LPU receive the details from the server to the smart phone.

C. Module 3: Data Authentication Module

In this module the User should login using the Android app in LPU and server verifies the user after the authentication, the LPU gets Connected with the body sensor network using Bluetooth, after the connection the project can receive data form the body sensor network and encrypts using the AES code block algorithm and the encrypted data is sent to the server. Server decrypts the data and checked the threshold value based on the range of the data collected, send alert to the family or to the local physician or an emergency care unit. In this module the LPU and Server mutually authenticate each other.

D. Module 4: Future Health Prediction

The collected data from the LPU by the BSN Care server is stored into the HDFS. The huge quantity of collected data are stored as soon as the data is received from the LPU. To predict the health condition of the patient, the data from the HDFS is retrieved and calculates the average health condition of the patient. Each time LUP updates the sensor collected data, embed the GPS location. Using Google location address provider we find out the current city and save the details in the HDFS. Form the collected data, we analyze and find out the better health condition city and recommend the patient.

BSN Body Temperature (BT) data	Action Required	Expected Response
BT<=28	NO Action	NULL
BT>32	Inform Family Members	FP=T/F
BT>32 & FR=F	Inform Local Physician	PR=T/F

BT>32, FR=F & PR=F	Inform Emergency	ER=T/F

FP=Family Response ;

PR=Physician Response

ER=Emergency Response

Table 2 Action Table for Body temperature

Table 2 shows Action Table for Body Temperature(BT).when the Body Temperature<=28F i.e (BT<=28F) no action is required and there is no expected response. When the Body Temperature >32F i.e (BT>32F) inform family members of the patient. When Body Temperature>32 i.e (BT>32) & there is no Response from family i.e (FR=F) then inform local physician. When Body Temperature >32 i.e (BT>32) & there is no response from family as well as from the physician i.e(FR=F & PR =F) then Inform Emergency Unit.

4. EXPERIMENTAL SETUP

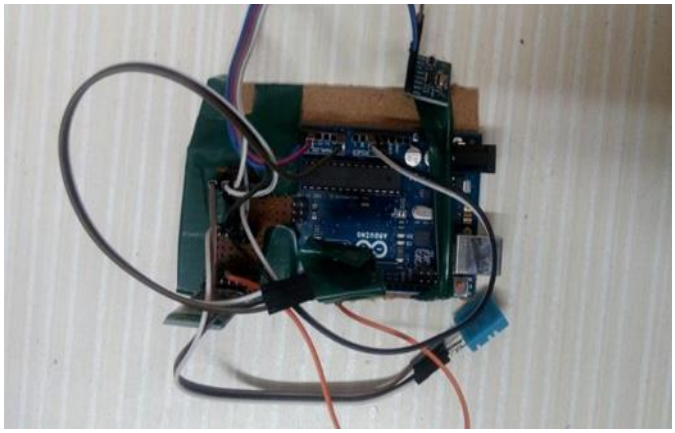

Figure 2 Hardware Setup of Arduino

Figure 2 shows The hardware setup of our proposed solution consists of Arduino board to which connect Bluetooth HC-05,different sensors like Temperature, Pulse and motion sensor for collecting patient data.

5. RESULTS AND DISCUSSIONS

In our approach first we have first collected the patient data using different sensors like temperature sensor, pulse sensor then we have paired the LPU (android phone) with the Bluetooth .Next the patient information is provided for registration and authentication. Any abnormalities in the sensor data will alert the family, physician or emergency unit through an SMS. Finally we have successfully predicted the average health condition of a patient by plotting graphs for Temperature and Pulse.

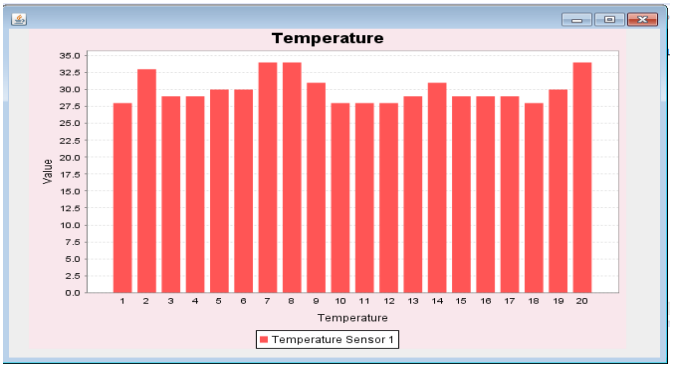

Figure 3 Temperature graph

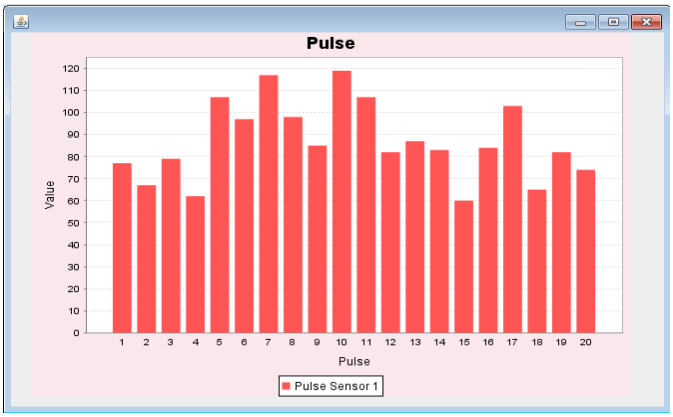

Figure 4 Pulse Graph

In Figure 3 & Figure 4 shows two graphs based on the temperature and pulse value recorded from the patient body. We have stored the data into HDFS. While plotting the graph we have collected the data from HDFS. An automatic intimation to the family or doctor is implemented via SMS.In case of body temperature, if the body temperature is below 28F or above 32F, a SMS alert is sent to the family or doctor along with the GPS location. In case of pulse, if the body pulse is below 72 or above 120, a SMS alert is sent to the family or doctor along with the GPS location.

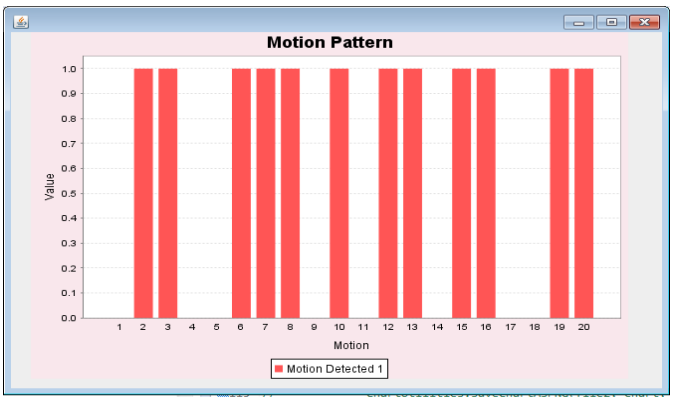

Figure 5 Motion Graph

In Figure 5 shows Motion pattern detected using Motion Sensor when Patient is in Motion.

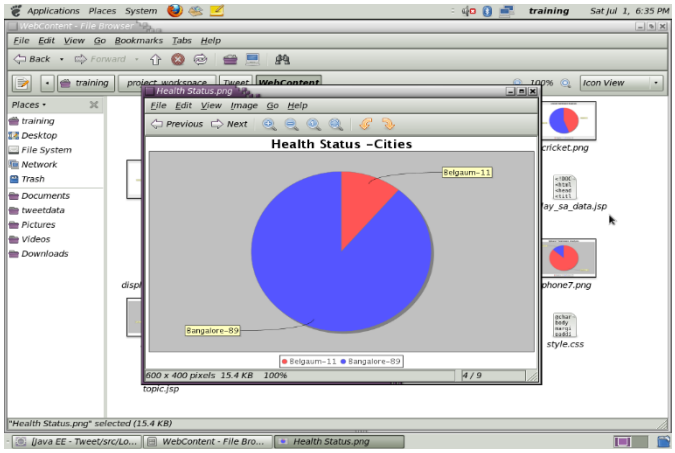

Figure 6 Pie chart for prediction of Health Status for different Cities

Figure 6 shows Pie Chart for Prediction of Health Status for Different Cities. From the collected data from the HDFS, we have plotted a pie chart. The input data are passed as input to plot the graph. The input is location and average health condition. We have gathered data in two different locations in Karnataka. Based on the plotted graph we can conclude that health condition is better in Bangalore, Karnataka than Belgaum, Karnataka.

6. CONCLUSION AND FUTURE SCOPE

In this article, at first we have described the security and the privacy issues in healthcare applications using Body Sensor Network (BSN). Subsequently, we found that even though most of the popular BSN based research projects acknowledge the issue of the security, but they fail to embed strong security services that could be used to preserve patient privacy. We have used LPU such as smart phone that will collect the data from the patient wearing sensors and forward this data to the BSN server. The collected data will be stored on HDFS Finally, we proposed a secure IoT based healthcare system using BSN, which can efficiently accomplish various security requirements of the BSN based healthcare system. In addition, Map Reduced based on HDFS file system model is used as the processing framework for our big data analysis. Each time LUP updates the sensor collected data, embed the GPS location. Using Google location address provider we find out the current city and save the details in the HDFS. Form the collected data, we analyze and find out the better health condition city and recommend the patient.

The system can be further enhanced by increasing the number of sensors for more accurate results. More sophisticated sensors, such as wireless sensors can be added to make the device more ergonomic and aesthetically pleasing. With the advancement in technology, this whole device can one day be scaled down in size in increase the ease in transportation.

REFERENCES

[1] D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, “CodeBlue: An ad hoc sensor network infrastructure for emergency medical care,” in Proc. MobiSys Workshop Appl. Mobile Embedded Syst. (WAMES), Boston, MA, USA, Jun. 2004, pp. 1–8.

[2] R. Chakravorty, “A programmable service architecture for mobile medical care,” in Proc. 4th Annu. IEEE Int. Conf. Pervasive Comput. Commun. Workshop (PERSOMW), Pisa, Italy, Mar. 2006, pp. 531–536.

[3] A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, “Caveat eptor: A comparativestudy of secure device pairing methods,” in Proc.IEEE Int. Conf. Pervasive Comput.Commun. (PerCom), Mar. 2009, pp. 1–10.

[4] Reliable Set-Up of Medical Body-Sensor Networks H. Baldus, K. Klabunde, and G. Müsch Philips Research Laboratories Aachen Weisshausstr. 2, 52066 Aachen, Germany