A Secure Health IoT for Patient Monitoring with Intelligent Medicine Box

Sonam V. Maju
Student, Department of Computer Science and Engineering
KMEA Engineering College, Ernakulam, India
Email:Sonammaju22@gmail.com

Abstract – An IoT application in the health platform is proposed here, which involves sensors for reading the human heart rate in digital format and an intelligent medicine box with a light sensor to indicate the variations in the medicine slots like counting the number of tablets a patient is consuming, alarms are there for consuming wrong medicine and more than that this medicine box will act as medication reminders. By largely using and promoting Home Health IoT the facilities and services of hospitals can be made available in our home environment itself.

Keywords – Bio-Sensors, Health-IoT, Intelligent Medicine Box, Internet-of-Things (IoT), Elliptical Curve Cryptography

I. INTRODUCTION

Currently, worldwide aging and regularity of persistent diseases are flattering a broad concern. Numerous countries are undergoing hospital restructuring by reducing number of hospital beds and escalating home healthcare, which is envisioned to perk up health care quality, has fascinated wide-ranging attention. In order to track the physical status of the elderly and, in the meanwhile, to keep them healthy, the proposed idea will be helpful.

IoT expands the Internet into our everyday lives by wirelessly connecting various smart objects , and will bring significant hangs in the way we live and interact with smart devices. The new wave in the era of computing will be outside the sphere of the conventional desktop. Internet of Things (IoT) is a network where many of the objects that surrounds us will be networked in one form or another. By using this technology the heartbeat sensors of the patient is collected through the heartbeat sensors and is fed to the computer server for processing and encryption. Thus this platform can continuously monitor the patient providing proper alarms and trigger a message when there is any abnormal variation in the pulse rate. The status of the patient is generated every day and is stored in the server in the encrypted format. The encryption algorithm used here is the arithmetic part of elliptical curve cryptography without generating a curve. This platform flawlessly fuse IoT devices with in-home healthcare services for an improved user experience and service efficiency.

The swift paced life has always taken a levy on the people. The satire is that new medicines are found for the never ending chain of diseases and often require timely medication with course therapy for curing. The existing techniques in market for the reminder include a pill box with a normal alarm. But this does not help in checking, overdose and wrong dosage among the patients. This proposed idea is a valuable solution to the medical non-compliance problem. Dropping patients non-compliance, guarantees better health, longer life expectancy, and better quality of life. The invention uses a dispensing scheme to help patients keep trail of their medicine consumption through a series of LED alarm indicator signals and audio alarm indicator signals.

II. LITERATURE SURVEY

Alok Kulkarni, Sampada Sathe’s [2] paper about healthcare internet applications, discuss about the evolution of internet, its concise discussion and applications. IoT is that network of physical objects or “things” fixed with electronics, software, sensors and connectivity to permit it to achieve higher values and facilities by exchanging data with the firm operators and other connected devices. Each objects around us are totally peculiar through its embedded computing system but is able to interoperate with the active Internet infrastructure.

David Niewolny in his paper describes, ‘How the Internet of Things Is Revolutionizing Healthcare’ [3] is discussing about the reasons for emergence of IoT and designs of applications where IoT is used. The issue is people have only limited time, awareness and accuracy, which means they won’t be able to capture data about things networked in the real world consistently. The answer is empowering devices to collect information on their own, without any human interference.

Different sensors are accessible and available in the market for providing ad ensuring home healthcare, S. Tozlu, M. Senel, W. Mao, and A. Keshavazirian in his paper[4] Wi-Fi enabled sensors for internet of things describes a practical approach,[4] and give explanations about different sensors available. Conventionally ZigBee and other IEEE 802.15.4 based protocols have been regarded for sensor network applications because of their energy-efficient design. On the other hand, newly developed power-efficient Wi-Fi components, with proper system design and usage model is a strong contender.

The terms ubiquitous and persistent computing designates the diffusion of our everyday life with intelligent devices. Security is significant for a diversity...
of sensor network applications. Public key cryptosystems are resource hungry but will provide a lot more features than confidentiality. Mathematical part of Elliptical Curve Cryptography (ECC) got the attention of the researchers due to its smaller key size. It guarantees practical implementation possibilities in resource constrained devices. Earlier work shows public key algorithms are best choice for use in wireless sensor networking, and that the advantage of smaller Cryptographic keys will be significant in getting better in energy conservation.

III. BACKGROUND AND FRAMEWORK

A promising trend in healthcare is to shift routine medical checks and other healthcare services from hospital (Hospital-Centric) to the home environment (Home-Centric). By doing so, first, the patients can get seamless healthcare at anytime in a comfortable home environment; next, society’s financial load could be greatly reduced by remote treatment; third, limited hospital resources can be released for people in call for of emergency care. In-home healthcare and services can drastically reduce the total spending on medical care or treatment. In order to track the physical status of the elderly and, in the meanwhile, to keep them healthy, the following two daily tasks are essential:
1) real-time monitoring and analyzing critical signs to early-detect or predict life-threatening difficult events;
2) checking whether they are following their prescribed treatment, with taking their prescribed medicine on time.

However, with rapidly aging populations, these daily tasks have brought immense pressure and confronts to global healthcare systems. One review estimates that about 25% of the adult population do not hold to their prescribed medication, which may lead to poor health outcomes and increased mortality. Poor medication adherence is a major problem for both individuals and healthcare providers. Technology upgrading in healthcare facilities and services are highly desirable to meet the requirements of this giant group.

Fig.1. Architecture of iHome Health System

With the emergence of wearable trackers today, there seems to be further ways than ever before to electronically detect a heartbeat, which sports a finger cuff with an integrated IR LED and photodiode. As blood is pumped through the body, the volume of blood in farthest points fluctuates with the beating of the heart. This change in blood volume in the finger tips can be sensed by shining a light through the finger and sensing the amount of light that passes in and out of the finger using a photodiode. Once the current produced by the photodiode is converted to a voltage by an amplifier and examined by the Arduino. This information is then passed on to a computer via serial.

To connect a sensor or a motor to an arduino, you require connecting them to its pins. The readings from the heartbeat sensor is fed into our system and is continuously monitored. The monitoring is done by reading these values from the .txt file and comparing the present pulse reading with the range pre-defined in the program. The normal pulse rate is being set and any variation from this normal value will trigger a message to the respective doctor and emergency center. The message set here is “Patient pattern become changing. Please provide ambulance service”, a period is set for sending the messages and the message will be send at these regular intervals.

Fig.2. Circuit Diagram of Heartbeat sensor

The Cryptographic method used here is the mathematical part of elliptical curve cryptography avoiding the geometrical part, as the geometrical part is not that so relevant in this criteria. It is a public key cryptography, where each user or the device, taking part in the communication normally use a pair of keys, a public key and a private key, and a set of operations associated with the keys will be undergone to complete the cryptographic operations. Crypto Algorithm, Crypto Analysis Secure key Management, Access control Authentication and secure routing Data Aggregation will be knowing the private key where the public key is circulated to all users taking part in the communication. Public-Key cryptographic systems are used to offer protected communications over timid channels without exchanging a secret key. The most admired public-key cryptography now is RSA and Elliptic Curve Cryptography (ECC).

IV. IMPLEMENTATION

A. HEARTBEAT TRACKING

The three pins of the heart beat sensors, which is the power pin, ground and input is connected to the 3.3v power pin, GND and A0 of the arduino board respectively.
Here Four light sensors are used which have two pins, one end is connected to the power and the other end is connected to the analog points of the board. The fifteen LED connection are connected to the digital pins and the Xbee is connected to the Transmitting and receiving serial pins. The transmission of data is done from the arduino board is wirelessly through one Xbee to the other, where one Xbee acts as the transmitter and other a the receiver. The receiver Xbee is connected to the system and the readings from the sensors can be seen in our computer screen. Further processing and analysis can be done in the software part.

![Fig.3. Overall Circuit Diagram](image)

The readings from the heartbeat sensor is fed into a file and is continuously monitored by reading these values from the file and comparing the present pulse reading with the range pre-defined in the program. The normal pulse rate is being set and any variation from this normal value will trigger a message to the respective doctor and emergency center. The atomatically generated message is “Patient pattern become changing. Please provide ambulance service”, an interval is set for sending the messages and this message will be sending at regular intervals.

A report will be generated on the patient’s condition for each day as a part of remote monitoring so that a doctor or even a responsible care giver can check the report on the daily basis and can take proper action if needed. The reports are generated based on the analysis of pulse rate obtained and several status is been already made and set, the corresponding status will be generated in comparison with the conditions set. If patient had a variation in his/her pulse rate then a status “pattern change is monitored” will be obtained. These status are not stored as such, the medical reports are always confidential and so these status are encrypted and stored.

The encrypted data will be stored in the server along with the number of report generated for the respective patient. The encryption method used here is the elliptical encryption, where a curve is not generated because here the geometrical representation of encryption method is not needed in this application. A doctor or a care giver can remotely check the status of the patient through this system. The status generated is stored in the server in the encrypted format which will be decrypted only when the doctor selects the patient’s report number. Doctor will get a list of reports generated on every day for the patient and doctor can select the report he/she wants from the list and the corresponding data will be decrypted in the server and the decrypted status will be displayed in the doctors profile.

**Encryption Algorithm**

E is the Public exponent and D is the Private exponent.P and the Q are two distinct large prime numbers.R is the big integer.

**Steps**

1. First generate prime number -
2. Generate public private key - (N = p * q (p, q are the big integer))
   \[ r = (p - 1) * (q - 1) \]
3. Compute D, the inverse of E mod r
4. Convert the message to bytes
5. Generate the array of big integer and its size is equal to message size
6. Convert each byte to big integer array
7. Generate the Cipher text - Calculate the big integers mode with E and M (Calculate Big Integer array whose value is (E mod M) this permits negative exponents)
8. Then convert the cipher to string
9. Encryption completed

**B. MEDICINE BOX**

The patient non-compliance is an important problem which places a prior importance to the health of millions of patients. The Medicine Box offers a solution to the patient non-compliance problem. The Smart Medicine Box keeps track the number and time of pills the patients have taken. This invention is therefore capable of improving patients’ health drastically. The functions of the Medicine Box are based on a LEDs and a microprocessor keeping track of time and amount of pills left in the Medicine Box. Patient’s schedule for taking his medication is also stored. The Medicine Box uses this information to infer whether the patient is complying with his treatment

(a) Medication Support

The device can hold more than one tablet/pill because the elderly and sick usually are prescribed with more than one medication to make them fit. The normal number of medications by each patient over the age of 60 years was greater than 5 per day.

(b) Dispensing Scheme

The medicine box have three LEDs of different colour, Green, Yellow and Red. Green LED indicates the ON mode of the medicine box. At the times of Medicines/ Pill to be taken as per the scheduled program respective LED indicator will give red flashing signal with a beep sound. This will indicate that the person had taken the prescribed tablet. If the box is opened after red signal then the yellow flashing LED will glow continuously no beep sound, indicating that the person is talking the pill. When the patient opens the medicine box, the light falls on the light sensor and it reads the value greater than 200 by flashing a yellow LED. If the pill box is closed, the value given by the sensor will be less than 200 at the same time respective LED indicator will give green flashing signal. Medicine Box records that pill has been consumed and sends the data to output system(personal computer). The total count
of the tablets in each slot will be stored in the system and each time when the patient consumes a medicine the number will be decreased from the total count. Once it is recorded that the pill has been taken the LED indication in front of the pill vial will glow continuously green till the next pill taken time as per schedule program. If the person tries to take the already consumed medicine within scheduled program time then medicine Box will give on the alert to the patient that this medicine/pill is not to be taken. Lastly when the next programmed time has been reached, the corresponding LED automatically flash the green signal with an audible alarm.

The 16 MHz crystal is used as the clock in arduino, it is essential for applications relating to timing, alarm etc. This will be used to make sure that the device gives alert sound to the user to take patient’s medication at the appropriate time, and that the medication is dispensed in a well-timed approach. The clock will be accurate. The time will be set upon system power up. The device has both sound and visual indications because the patient may have either a hearing or sight impairment. When it is time to take the medicine, a single LED will blink and the buzzer of the device will give an alarm, and the LED will flash.

(c) Software approach

Programming is done in the Arduino IDE by using several flags and conditions. Three LEDs have to blink only if they satisfy the conditions, the green light will be ON always so as to make sure that the system is in working condition and an initial flag will be set for this stage. The red light blinks at the prescribed time along with green signal and a new flag say is set in this condition, this red light act as a reminder for taking medicine. Now, when the patient opens the box, the light falls on the sensors and if the reading of the sensors is greater than 960 and the rf flag is set, then a yellow LED blinks which represents the box is opened for taking the medicine, and another flag will be set for this condition. If the recently set flag and the light sensor reading is less than 960 then the yellow LED will be in OFF mode and this shows that the box will be closed. The flashing of the yellow LED can be used to count the medicines consumed. Each time when a yellow LED is flashing ON and OFF, the count will be decreased by one from the total count and a message will be displayed like “medicine count in box B”. At the same time, if the patient opens the wrong medicine box, the conditions and flags didn’t match properly and a message indicating “wrong medicine box opened” will be shown along with a continuous blinking of red LED with an alarm.

VI. CONCLUSION AND FUTURE SCOPE

An IoT-based intelligent home-centric healthcare IoT platform, which flawlessly connects smart sensors attached to human body for biological monitoring and intelligent medical packaging for daily medication management. It includes the scenario of assisted living for people with physically and mentally disabled, where users can intermingle with smart objects deployed in a home environment to ensure their health and well-being. The proposed Home health system involves different aspects from the hospital, emergency center, body, and even medicine. The MedBox serves as a home healthcare station providing strong interoperability and network connectivity. The healthcare system can deliver various services, including monitoring of real-time bio-signals, alarms and medication noncompliance control. The Health system combines the health network, telemedicine, and emergency and medication management services. This helps in the swift transformation from Hospital-Centric medical treatment to Home-Centric healthcare and finally bring about ubiquitous and personalized healthcare.

Today, the most widely adapted technology for the Internet is the standard web services. Wireless identifiable embedded healthcare systems at the edge of the network should be connected to web services and make use of comparable functionalities and this will prove to be a challenge in the future for the internet. These millions of components produce, analyse, consume and process information in dissimilar healthcare environments such as hospitals, households and nursing homes as well as in the work and everyday lives of people. The Internet of Things will change our society, and will bring seamless ‘anytime, anywhere’ personalized healthcare and monitoring over fast reliable and secure networks. This implies that we are approaching the end of the divide present between digital, virtual and physical worlds.

REFERENCES

[1] Geng Yang, Li Xie, “A Health-IoT Platform Based on the Integration of Intelligent Packaging, Unobtrusive Bio-Sensor, and Intelligent Medicine Box”, IEEE transactions on industrial informatics, vol. 10, no. 4, november 2014, Matti Mäntysalo, Xiaolin Zhou, Member, IEEE, Zhubo Pang, Li Da Xu, Senior Member, IEEE, Sharon Kao-Walter, Qiang Chen, and Li-Rong Zheng, Senior Member, IEEE


