ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

IOT Based Secure and Efficient Health Care Management System

[1]Dr.R.S.Ponmagal, [2] Dr.K.Sujataha, [3]U.Indumathi [4]R.Aiyshwariya Devi, [5]T.Yuvarani
[1][3][4][5] Department of CSE, [2] Department of EEE,
Dr.M.G.R.Educational and Research Institute University, Chennai, India
[1]rsponmagal@gmail.com,[2] drksujatha23@gmail.com, [3]indumathi.cse@drmgrdu.ac.in,
[3]aishwariya.cse@drmgrdu.ac.in, [3]yuvarani.cse@drmgrdu.ac.in

***Abstract*— Internet of Things (IOT) based healthcare systems includes embedded devices such as sensors that are connected directly with each other to gather vital data and deploy the data in cloud. Sensors implanted in patients and communication of sensor data using IEEE 802.15.4,GPRS/GSM and HTTP is underpinning technologies of IOT deployments in the healthcare systems. It is proposed to analyze the securely captured patient health data from a variety of sensors using complex algorithms. Health proxy is proposed to securely store the health data in the cloud, where it can be accessed by physician. The health proxy captures patient data from a variety of sensors and in this paper, a patient's heart beat and finger moisture levels are sensed through suitable sensors and planned to transmit these data to a physician using GPRS/GSM. To facilitate sturdy security practicalities for the ubiquitous IOT such as proposed health care systems, plethora of factors need to be taken into account. For example in this paper data security, privacy, access control, seamless integration and system heterogeneity are considered. The health care management is accomplished by triggering an alert in physicians monitoring system when the monitored parameters are reaching the dangerous level while taking secure communication into consideration.**

***Index Terms*— health proxy, IOT, security, sensors**

I. INTRODUCTION

The Internet of Things entails the escalating dominance of objects and entities known as things and are endowed with unique identifiers and have the facility to transmit data over a network automatically. To a great extent of the increase in IOT communication [1] comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices.

"Thing" , in this paper is a person with a finger moisture sensor and heart beat monitoring sensor. Proposed IOT- based secure healthcare systems, comprises:

- Sensors that collect patient data
- Microcontrollers that process analyze and wirelessly communicate the data
- Healthcare proxy (IOT Agent) through which sensor data is further analyzed and to securely store them to the cloud
- Processors (monitors) that facilitate graphical user interfaces

People affected with Sjögren's syndrome (causes dry eyes and mouth; a type of autoimmune disease)[2] are also associated with Peripheral neuropathy, this causes loss of sensation in fingers, hands, arms, toes, feet, and legs. Reynaud's phenomenon [3] is where the extremities of the body, usually the fingers and toes, change colour and may become painful, usually due to exposure to the cold. Hence in this paper, monitoring a patient with above disease is carried out with the finger moisture sensor. The cloud makes it possible to collect record and analyze vital data streams faster and more accurately. These types of monitoring systems demonstrate how all things such as patients, physicians, emergency services, and healthcare facilities can be connected and used to extract the important value from available, real-time data.

Security experts have warned of the potential risk of large numbers of unsecured devices [1] connecting to the Internet since the IOT concept was first proposed in the late 1990s.To improve security, an IOT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be monitored to identify potential anomalous traffic, and action should be taken if there is a problem.

The physician could provide emergency medication suggestion through his mobile phone. Also, it is

proposed to make these data available in cloud and health care (historical analysis) is monitored from cloud. As cloud could support in managing increasing volume of health data in medical engineering, professionally share the information across health care systems, bring down operational and management costs and could provide reasonable health care services, in this paper, Intel Galileo gen 2 which plays the role of IOT agent to deploy the medical data in to cloud is proposed and implemented. The response time is found to be less and hence the performance of the proposed system is improved with the existing remote health monitoring system.

This paper is organized as follows: Section II describes the recent trends in health care systems in IOT. Section III details the proposed system. Section IV details the materials and methods used for implementation. Section V describes the evaluation analysis. Section V concludes the paper.

II. STATE OF THE ART

In order to circumvent the problem of security in IOT domain [4], networks and devices need to be secured. This paper, considers the embedded device security only, assuming that network security is properly in place. The security issues of the Internet of Things (IOT) are directly related to the wide application of its system. Beginning with introducing the architecture and features of IOT security [5], this paper expounds several security issues of IOT that exist in the three-layer system structure, and comes up with solutions to the issues above coupled with key technologies involved.

This paper [6] gives a detailed survey and analysis of embedded security, especially in the area of IOT. Together with the conventional security solutions, the paper highlights the need to provide in-built security in the device itself to provide a flexible infrastructure for dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful breaches. Based on this survey and analysis, the paper defines the security needs taking into account computational time, energy consumption and memory requirements of the devices.

Security and privacy are the key issues for IOT applications [7], and still face some enormous challenges. As security will be a fundamental enabling factor of most IOT applications [8], mechanisms must also be designed to protect communications enabled by such technologies. This survey analyzes existing protocols and mechanisms to secure communications in the IOT, as well as open research issues.

There are no standards or regulations to govern about the information collected via the IOT [9]. A guide is prepared by the national institute of standards and technology to secure connected medical devices. Empowering health monitors [10] and patient devices with internet capabilities are available; however there is a lack in service intelligence in generic m-health scenarios.

A pulse oximeter prototype is introduced in a paper [11] which is designed for mobile healthcare. In this prototype, a reflection pulse oximeter is embedded into the back cover of a smart handheld device to offer the convenient measurement of both heart rate and estimation of arterial oxygen saturation for mobile applications.

A paper [12] proposes an original, IOT-aware, smart architecture for automatic monitoring and tracking of patients, personnel, and biomedical devices within medical institutes. Fastest to espouse the internet of things is the healthcare industry [13]. The motive for this inclination is that incorporating IOT features into medical devices significantly advances the quality and efficacies of service, bringing particularly high value for the elderly, patients with chronic conditions, and those have the need of constant supervision. IOT-related healthcare systems nowadays are based on the fundamental definition of the IOT as a network of devices that connect directly with each other to capture and share vital data through a secure service layer (ssl) [14] that connects to a central command and control server in the cloud.

III. PROPOSED SYSTEM

We mainly introduce the design of a heterogeneous IEEE 802.15.4 based personal health device monitoring system which consists of different health monitoring sensors, such as finger humidity and heart beat rate sensors. The health monitoring sensors are touched by human to sample the physiological signals of the people.

Proposed IOT system architecture is shown in figure 1. Body sensors such as humidity sensor implanted in the finger and heart beat sensors are connected with IOT agent. IOT agent acts as health proxy. The IOT agent is supplemented with security chip which verifies the authentication of the medical parameters deployed. The sensed information could be deployed in to cloud for further historical analysis of health parameters of a particular patient.

The sensors and other devices connected to the internet of things often store sensitive user data, here the health parameters of a particular patient locally. Patients might have concerns that this data could be accessed or manipulated over the IOT. These data privacy uncertainties

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

can be lessened by encrypting the data and hence protecting its integrity and confidentiality.

Apart from these kinds of personal user data, decryption keys, authorization codes, critical parameters and logs are also stored in the sensor devices. Some of this data is confidential (e.g. Media decryption keys) and much of it requires integrity protection (e.g. Monitored parameter logs at different times).the challenge in ensuring data privacy and integrity protection lies in securely storing cryptographic keys.

The security chip supplemented with IOT agent also does the job of mutual authentication between the cloud server and the communication network. The security chip receives the health parameters from IOT agent, encrypts it and returns the decrypted parameters on request. The encryption algorithm used here is elliptic curve cryptography with 163 bit key length which is an asymmetric key cryptographic algorithm. Further it enables a session key feature, which further enhances the security of the system. The monitoring system could collect health data from cloud with appropriate gateway. Hence the proposed combination of device level security and network security provides a robust authentication solution and enables a trusted relation among the devices and networks. The secure communication could be established using hardware-based security by way of storing the keys used in communication protocols implemented in the microcontroller coming with the IOT agent. The security chip proposed would generate and securely store encryption keys for one-way and mutual authentication, thus protecting devices and networks against malware and controlling access. The function of the proposed security chip includes secure storage of cryptographic keys. Further the security chip is supplemented by software and hardware integrity checks to prevent the cryptographic keys from falling into attackers' hands.

The mobile phone of the physician could be directly connected with IOT agent using GPIO pins. The physician could provide support in case of emergency situation of patients, i.e., if heart beat rate exceeds the recommended value, an alert could be generated from the physician for proper medication suggestions. Alternatively the health monitoring system could also be connected with the mobile phone.

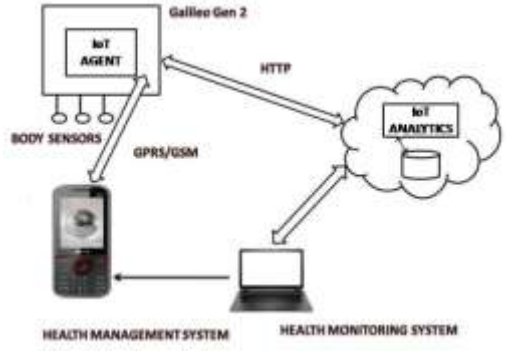

Fig. 1. ***Proposed IOT Architecture***

The system proposed, deliver intelligence where needed to acquire and deliver health data securely. Billions of such intelligent devices could share data and securely supporting legacy and new environments through the proposed system. The system provides connectivity from digital sensor device to cloud to deliver end to end customer (patient – physician) value.

IV. MATERIALS AND METHODS

As, Intel Galileo is now officially registered device under IBM Internet of Things Foundation (IOT Foundation), it is selected for implementation. Arduino programming for Intel Galileo Gen2 is done to record the sensor values. Sensors are used for health care data collection. Interfacing with physical world such as digital sensors, GPRS/GSM, and I2C is possible with Intel Galileo Gen2, and hence it is chosen for implementation. Fig 2 and 3 shows the heart beat sensor and moisture sensor in the proposed work.

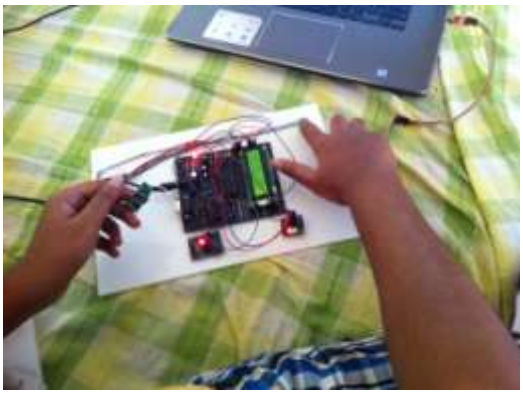

Fig. 2. ***Heart beat sensor with IEEE 802.15.4 sender and receiver***

ATWIN Quad-band GPRS/GSM [15] shield has PCB etched antenna, so no need for external antenna.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

ATWIN Quad-band GPRS/GSM shield is an ultra compact and high quality wireless module base on Infineon UCL2 platform with industry-standard interface. This is a SMT package with small dimension, low power consumption, quad-band (AT139) and dual-band (AT139D) GSM/GPRS module. It can provide with voice, SMS, Fax, data applications for customers. Figure 4 shows this.

- Rx of hardware serial port is connected to Galileo's D0.
- Tx of hardware serial port is connected to Galileo's D1.
- 5V of hardware serial port is connected to Galileo's 5V.
- GND of hardware serial port is connected to Galileo's GND.

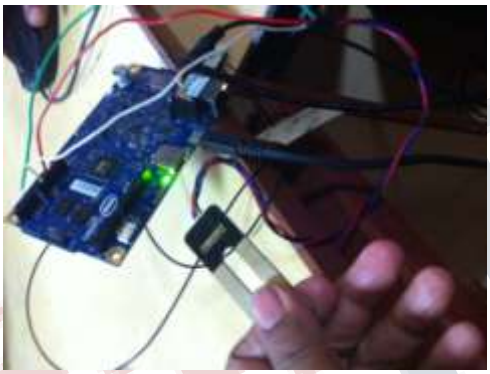

Fig. 3. ***Moisture sensor with Intel Galileo Gen2***

Insert an unlocked SIM card. The SIM is a mini-SIM or 2FF size. Attach the shield to the Galileo. There is no extra wiring necessary. Set the Serial port select jumpers to the Hardware Serial position:

- Set J1 so that Rx is connected to MTx.
- Set J2 so that Tx is connected to MRx.

Figure 5 shows the SIM card inserted into Intel Galileo.

Fig. 4. ***SMT package inserted into Intel Galileo with PCB antenna***

The Intel IOT developer kit used in this paper includes the required components to connect the intelgalileo board to the internet via Wi-Fi. Intel Galileo gen2 also offers the connectivity of sensors to cloud with the Wi-Fi support through menisci slot available; leading to IOT based health care system. Intel provides end to end IOT solutions so that one could quickly connect, manage, and protect the digital sensors.

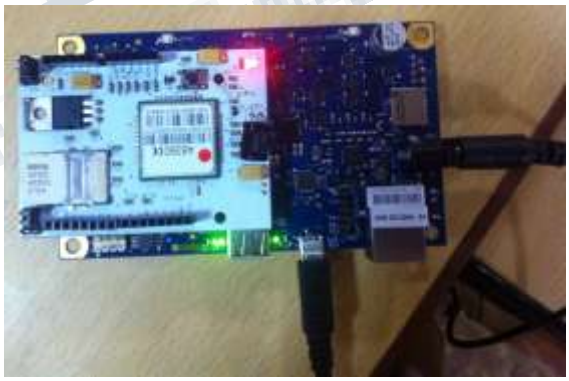

Fig. 5. SIM Card inserted to Galileo Gen2

After establishing the Wi-Fi connections with necessary commands, the gathered physiological parameters such as finger moisture level and hear beat rate levels using sensors are stored on a web server (cloud) for further processing and sharing with physicians. in this paper, " thing speak" cloud is chosen. Initially, a new user account is created and a new channel is created by selecting available channels. Write api key is entered using http post method to deploy the sensed data in to the cloud. Figure 6 shows the finger moisture

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

deployed in “thing speak” cloud, and it shows the recording of moisture value at various time intervals.

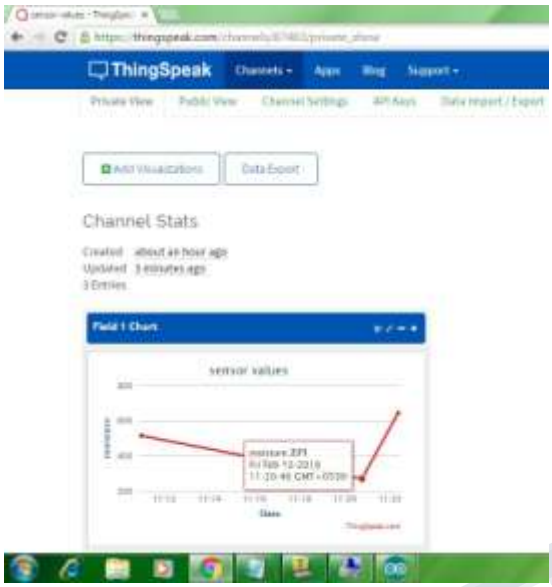

Fig. 6. ***Finger moisture deployment in Thingspeak cloud***

V. RESULTS DISCUSSION

The heart beat rate monitoring is accomplished by making the person (whose heart rate to be monitored) to press the sensor, and it starts transmitting heart beat data and this is deployed in Thing speak cloud through IOT agent similar to the moisture sensor shown in figure 6. From the cloud the information goes to the monitoring interface which is shown in figure 7 and 8. From the interface the mobile phone could be connected. Alternatively the IOT agent is connected to the mobile phone with SMT package and SIM card inserted to it.

The alert system is based on threshold calculated as shown in Figure 8. The proposed system is designed to send alert message instantly, once arrhythmia is detected. The system has also the ability to notify the conditions of tachycardia and bradycardia. The alert messages are generated at mobile phone as shown in figure 9. Extracted physiological parameters give the alert signals after comparison with assigned threshold [16] values. These alert signals indicate aberration such as arrhythmia. The proposed system contains adaptive alert system which generates alerts to notify the concerned physician in case of emergency.

Fig. 7. ***Health monitoring of Interface***

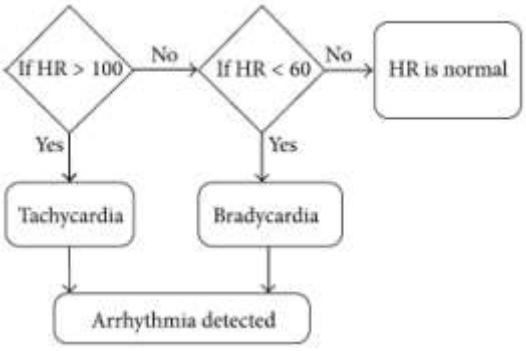

Fig. 8. ***Flow chart for alert***

The following AT(attention) commands are used to send a SMS to physician mobile in Text mode

"AT+CMGF=1\r" To add the receiver (physician) no.

"AT+CMGS=\"09698433804\""

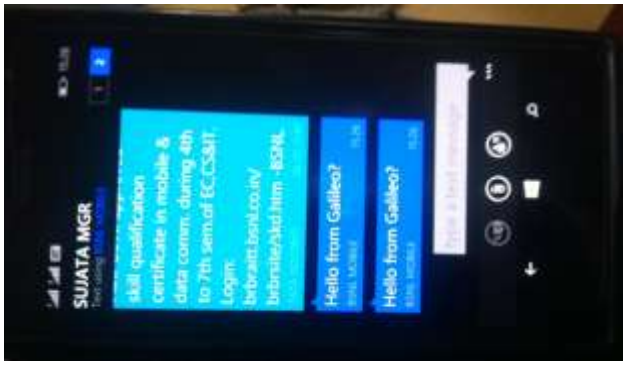

Fig. 9. ***Alert interface of health monitoring system.***

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

Table i shows the threshold values for the alert for heart beat rate. Table ii shows the recordings of the heart beat alerts in the proposed iot based health monitoring system. It is compared with the existing system [16], and it is found to provide the alert with lesser response time, and hence the performance of the proposed system is improved as for as the heart beat rate monitoring is concerned.

TABLE I THRESHOLD VALUES FOE ALERT

Alert for	*Average time b/w sending and receiving alert in Wi-Fi (H:M:S)*	*Average time b/w sending and receiving alert in 3G network (H:M:S)*	*Average time b/w sending and receiving alert in proposed IoT system (H:M:S)*
Tachycardia	00:00:29	00:00:58	00:00:25
Bradycardia	00:00:30	00:00:59	00:00:28

Table II AVERAGE DATA TRANSMISSION TIME

Sinus rhythm type	*Threshold value of heart rate)*
Normal	60 ≤ HR ≤ 100 (beats/minute)
Tachycardia	HR ≥ 100 (beats/minute)
Bradycardia	HR ≤ 60 (beats/minute)
Sinus rhythm type	*Threshold value of heart rate)*
Normal	60 ≤ HR ≤ 100 (beats/minute)
Tachycardia	HR ≥ 100 (beats/minute)
Bradycardia	HR ≤ 60 (beats/minute)

Note: the value for each type of alert is the average value of 20 alerts.

VI. CONCLUSION

Health monitoring parameters such as finger humidity and heart beat rates are considered and monitored after secure authentication. The proposed work provides peace of mind for end users with stronger hardware security (Security chip) and reduced risk of attacks in IOT Communications. "Things peak" cloud is used to monitor the health parameters using IOT agent. In this paper data security privacy, access controls of health parameters are achieved through security chip.

The management of health parameters is executed by means of alert messages through mobile phones using GSM/GPRS connection possibilities of the IOT agent. The monitoring (raising alert message when the stipulated threshold reaches) response times are compared with previous methodologies and found to be improved

REFERENCES

1) http://internetofthingsagenda.techtarget.com/definition/IOT-security-Internet-of-Things-security
2) https://www.healthtap.com/topics/symptoms-usually-affect-fingers-toes-nose-lips-or-earlobes
3) http://patient.info/health/raynauds-phenomenon-leaflet
A. Ukil , J. Sen ; S. Koilakonda, "Embedded security for Internet of Things", IEEE 2nd National Conference onEmerging Trends and Applications in Computer Science (NCETACS), 2011,pp.1-7.
4) Kai Zhao , Lina Ge, "A Survey on the Internet of Things Security", IEEE 9th International Conference on Computational Intelligence and Security (CIS),2013, pp.663-667.
5) S. Babar, Aalborg, A. Stango ; N. Prasad ; J. Sen , "Proposed embedded security framework for Internet of Things (IOT)", IEEE 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE),2011, pp.1-5.
6) H. Suo ; J. Wan ; C. Zou ; J. Liu, "Security in the Internet of Things: A Review", International Conference on Computer Science and Electronics Engineering (ICCSEE), (Volume:3),2012,pp.648-651.
7) J. Granjal , E. Monteiro ,J. Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials (Volume:17 , Issue: 3),2015, pp. 1294 - 1312.
8) Andreas K. Triantafyllidis, Carmelo Velardo, Dario Salvi, Syed Ahmar Shah, Vassilis G. Koutkias, and Lionel Tarassenko, A Survey of Mobile Phone Sensing, Self-reporting and Social Sharing for Pervasive Healthcare,DOI

10.1109/JBHI.2015.2483902, IEEE Journal of Biomedical and Health Informatics, 2015.

9) S. M. Riazul Islam , Daehan Kwak ; MD. Humaun Kabir ; Mahmud Hossain, "The Internet of Things for Health Care: A Comprehensive Survey" , IEEE Access (Volume:3), pp. 678 – 708,2015.
10) Zhiyuan Lu, Xiang Chen, Zhongfei Dong, Zhangyan Zhao, Xu Zhang, "A Prototype of Reflection Pulse Oximeter designed for mobile health care, DOI 10.1109/JBHI.2015.2465861, IEEE Journal of Biomedical and Health Informatics, No. of pages 12, 2015.
11) Alexandros Pantelopoulos,Nikolaos G. Bourbakis, "A survey on wearable sensor-based systems for health monitoring and prognosis" ,IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews , Vol. 40 Issue 1, Pages 1-12, 2010 .
12) How the Internet of Things is changing healthcare and transportation http://www.cio.com/article/2981481/healthcare/how-the-internet-of-things-is-changing-healthcare-and-transportation.html
13) S. M. Riazul Islam , Daehan Kwak ; MD. Humaun Kabir ; Mahmud Hossain, "The Internet of Things for Health Care: A Comprehensive Survey" , IEEE Access (Volume:3), pp. 678 – 708,2015.
14) https://www.openhacks.com/page/productos/id/546/title/ATWIN-Quad-band-GPRS-GSM-Shield-for-Arduino
15) Priyanka Kakria, N. K. Tripathi,and Peerapong Kitipawang," A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors" ,International Journal of Telemedicine and Applications Vol. 2015 (2015), Article ID 373474, 11 pages, http://dx.doi.org/10.1155/2015/373474, 2015.