A Modern and Secure Healthcare System based on IoT – BSN-Care

Miss. Anushka Shailesh Shrivastava[1] Prof. Rahul Paikrao [2]

P.G.Student,Departmentof Computer Engineering[1], Head of Department, Department of Computer Engineering[2], Amrutvahini College of Engineering, Sangamner,MH,India[1] Amrutvahini College of Engineering, Sangamner, MH, India[2]

Abstract: ***The advancements in communication technologies of modern smart objects bring with them a new era of application development for IoT based networks. Particularly, due to the contactless nature and efficient data retrieval by mobile & smart objects, such as wearable smart watches or tailored biological sensors, several types of innovative healthcare systems including body sensor networks (BSN) have been proposed. Advancements in communication technologies have led to the emergence of IoT. In the modern health care environment, the usage of IoT technologies brings convenience of physicians and patients since they are applied to various medical areas (such as real-time monitoring, patient information management, and healthcare management). One of the core technologies of IoT developments in healthcare system is the body sensor networks. A patient can be monitored with a collection of tiny, powered and light in weight wireless sensor nodes. To simultaneously achieve system efficiency and robustness of transmission within public IoT-based communication networks, we utilize robust MQTT – Message Queuing Telemetry Transport protocol as the communication mechanism among smart objects- the sensors, the processing unit and the BSN server.***

Keywords: Internet of Things (IoT), Body sensor network (BSN), Wireless sensors, Security.

I. INTRODUCTION

IoT has transpired out of advancements in communication technologies. Applying the IoT technology in day to day appliances brings a convenience. Body Sensor Networks is a core IoT technology in healthcare systems. The monitoring of a patient can be done using wireless biological sensors. Different devices can interact seamlessly among themselves using IoT. A recently published report by United Nations (UN) has made the predictions that by 2050, from the entire population in the world about 22 percent will be of the people of older age. To add to it, a research has recently indicated about the likelihood of the older people living independently is around 89 percent. Nevertheless, a survey based on a research has found that around 80 percent people of older age (i.e. older than 65) would most likely get affected by one or more fatal disease. It might result in difficulty in their self-care. Presently, providing a satisfactory and acceptable life to the older aged people socially is one of the challenges. The communication and information technologies have grown drastically over the years. This has led to an innovation in healthcare solutions and tools that promise in addressing of the challenges. In the 21st century prototypes of communication the most prominent is the Internet of Things. Due to their efficient computing and communication capabilities all the daily life objects are becoming a part of the internet environment of the IoT, which is inclusive of micro controllers and transceivers for digital communication. Conceptually the internet is extended by IoT and made comparatively widespread. Various devices such as the home appliances, monitoring cameras, the medical sensors and the likes can seamlessly interact through IoT.

II. LITERATURE SURVEY

Various researches and projects concerning healthcare using wireless technology have been recently proposed. These projects are aimed at providing in-ambulatory, in-clinic, continuous and open environment patient monitoring. As the technology of BSN has advanced in the environment of healthcare and applications, patient monitoring has become more feasible. The section below describes the relevant research projects that have been prominent in healthcare applications in BSN[1].

CodeBlue[2], based on BSN was developed at Harvard Sensor Network Lab is a popular healthcare research project. Multiple biological sensors are positioned on the patient's body. The end user's device like PDAs, personal computers, mobile devices or laptops receive the data sensed by the sensors on the body of the patients. The transmission occurs through wireless mediums. CodeBlue's authors have acknowledged the need of security in medical applications. However the issue of security is yet to be resolved or they might have left the security requirements to be considered in future. Basically the CodeBlue implies to a categorical idea where a medical professional or a doctor with the help

their end user device states a query regarding the health of the respective patients. It is based on the publish – subscribe mechanism.

The Virginia University designed a heterogeneous architecture of a network and named it Alarm-net[3]. The purpose of the research was to particularly monitor the health of the patient in homely environment as well as in assisted living ambience. In addition to sensor networks of body Alarm-net also includes sensor networks of environment. The circadian activity rhythms program has been developed by the authors to provide a context aware policy of management of power and privacy. Further the data security and network security related to the residents is provided by Alarm-net for the parameters like environment, physiology and behavior. Some scenarios about confidentiality infringement on Alarm-net like susceptibility to confidential information attack results in the leakage of information of resident's location.

The department of computing in Imperial College, London proposed a system named UbiMon[4]. The project aimed at addressing the issues respective to the application of implantable as well as wearable sensors used for mobile monitoring in distributed manner. There is no specific need of considering the security related to health monitoring wirelessly which holds prominence in these applications.

For a timely and continuous monitoring of the status of a patient's physiology MobiCare[5] facilitates a widespread system for monitoring. MobiCare deals with security issues acknowledged by developers. However mere acknowledgement is not enough for the applications regarding real-time healthcare. The developers of the system have left the privacy as well as security requirements to be considered in future. In addition to these, other requirements like anonymity, secure localization, etc are not given any consideration in the system.

The system called Median[6] was developed at University of John Hopkins. It is specifically meant for monitoring of the patients not only in the hospital but also in the events like disasters. It incorporates multiple physiological monitors (called PMs), battery powered nodes and the medical sensors collect the patient's health information like pulse rates, oxygen levels in the blood. The description of Median states acknowledgement of authors regarding the encryption requirement for PMs, but they have not mentioned as of which encryption system has been applied for maintaining the integrity and privacy of the received data. Certain properties of security have been included into Median, though the authors did not describe much related to the implementation of security.

III. PROPOSED SYSTEM OVERVIEW

The Body Sensor Network technology congregates many kinds of biological sensor nodes that are low-powered and intelligent on and around the body of humans. The nodes trace the functions of the body as well as the environmental and surrounding events. Potentially, the present healthcare technology and its future can be revolutionized greatly by the BSN technology. Basically, BSN comprises of in-body and on-body biological sensor networks. The sensors that are planted on the human body can establish a connection between the devices/subscribers and the base station. In the architecture of BSN-Care system there are wearable biological sensors. These biological sensor nodes are integrated with biological sensors like heartbeat sensors, temperature sensors, blood pressure (BP) sensors, electro cardio graph (ECG) sensors, etc. These sensors then collect their respective information to forward it towards the coordinator LPU-Local Processing Unit. The LPU in our BSN-care system is the Raspberry Pi3 processor. The sensor nodes and the centrally located server i.e. BSN-Care server are mediated by the processor (LPU). Here, communication requires a broker for publish/subscribe mechanism. Here, the MQTT broker will be used to accomplish the communication between the subscriber and publisher of the message. The patient/person wearing the bio-sensor is provided an immediate alert as soon as any abnormalities are detected by the LPU.

We know that the normal blood pressure is either 120 or less than that. However if blood pressure reaches, say, 125 an initial alert is provided to the patient/person via the LPU device. Upon receiving the data of the respective person who is wearing the bio-sensor, the server then feeds the sensor data to the database for storing it and analyzing it. The result is, the server may decide to interact either with the person's family members, the locally available physician, or if required even the emergency services available nearby. The server decides upon the interaction action depending on the grade or level of the abnormalities of the patient/person. In the case where the person may be a normal person, i.e. who is not necessarily a patient, and is wearing the bio-sensors, can send and receive regular periodic updates through the sensor-LPU-server communication. We can thus say that the BSN-Care system is not only meant especially for the patients but also is also useful for normal people who wish to take care of their health. Not to mention that BSN-Care can be greatly useful to provide a satisfactory and acceptable quality of life to the older aged people.

The proposed system is mainly designed for real-time health monitoring that provides healthy life and timely care through emerging technologies. The system comprises of the following major parts:

1. Medical Sensors: Vital signals such as temperature, pressure, ECG, Blood Pressure and heartbeat are periodically measured from the patient by using respective sensors.
2. Processing and Analyzing: These vital parameters are analyzed against the health standards to detect any abnormal conditions of the patient who is being monitored.
3. Alert assurances: In case of any abnormalities, alert messages to the doctor and caretaker will be viewed through the dashboard, web interface or mail notifications.

The real-time data can be gathered through the sensors and transmitted through MQTT protocol. The data is published to the MQTT client/subscriber. The broker - Mosquitto communicates the messages among all the clients. The data thus collected is then stored at the back-end client database to be analyzed further to predict the anomalies on timely basis and to provide timely medication. The end user dashboard can be made up by subscribing to the collected data from the MQTT client and this data is then displayed in an interactive mode where all the subscribers can comprehend the health status easily. The notification regarding the patient's current health status can be conveyed to the doctor and the caretaker if required for further treatment through mail. The dashboard can be seen either on a web server or Mobile API. The patient's location is supervised and this guarantees that the patient can be reached out in case of any emergency kind of situations. The patient's health status can be tracked through the dashboard regularly to improve the health conditions of the patients. A daily health tip can be updated to the subscribers based on the health conditions of the patients.

IV. ALGORITHMS DESIGN

The Message Queuing Telemetry Transport protocol is a decent choice for wireless network communications which go through varying levels of latency because of occasional bandwidth restrictions or unreliable connections. MQTT protocol is based on the publish-subscribe pattern. The MQTT broker is the key component in the protocol and dispatching messages to the MQTT clients i.e. subscribers is the main function of the broker. In case where the connection from a subscribing client to a broker is interrupted, the broker will push the messages by buffering them out to the subscriber when it gets back online. And whenever the connection from the publishing client to the broker gets disconnected unnoticeably, the broker can terminate the connection. The broker then sends the subscribers a message containing instructions from the publisher.

Given the HTTP protocol, a request/response mechanism is used for communication mechanism for all the devices that make a connection to the IoT Agent. MQTT differs in this way that it uses publish-subscribe mechanism and is event-driven and pushes messages to clients.

A session of MQTT is divided in four distinct stages:

1. **Connection** - An MQTT client and broker establish the connection using CONNECT message. But there is no way to establish a direct connection amongst the clients. The client has to send the CONNECT message to the broker to establish the connection with it.
2. **Authentication**
3. **Communication**
4. **Termination** - The established connection between the clients and the broker is kept open by the broker unless a DISCONNECT command is received or unless the connection breaks for a reason.

A client starts by creating a TCP/IP connection to the broker by using either a standard port or a custom port defined by the broker's operators. When making the association, it is necessary to acknowledge that the server may continue a recent session if it is given a reused consumer identity. The standard port 1883 is for non-encrypted communication and the port 8883 for encrypted communication by exploiting SSL/TLS. To authenticate the server, the client validates the server certificate during SSL/TLS handshake. The broker can use a client certificate provided by the client for authentication during the handshake. It is necessary for the brokers to support client authentication using the SSL/TLS certificates. As the MQTT protocol intends to be a mechanism for resource-constrained devices as well as IoT devices, sometimes the SSL/TLS is not always as alternative. In cases like these, authentication is conferred as a username-password which is sent by the subscriber to the broker as a part of the CONNECT message packet. Some

brokers, particularly open brokers revealed on the web, can settle for anonymous subscribers. Here the username and password are just left blank. MQTT is termed a light-weight protocol as a result of all its messages have a little code footprint. Each message has a definite header of 2 bytes which is an optional variable header, a payload which is of 256 MB and a QoS level. There are three distinct QoS levels that determine in what manner the contents are organized by the protocol. We know that higher the level of QoS, higher is the level of reliability but they require higher latency and bandwidth. Thus the subscribers can mention the level of QoS that they would desire. MQTT suits well for the applications of IoT devices that use M2M communication mechanism. These find applications in smart homes, industry and manufacturing, logistics, medical and healthcare applications and more environments like these.

V. CONCLUSION

Various security requirements of healthcare system can be efficiently accomplished using BSN-Care. The cost of the system developed using such technology is user acceptable. It can be largely beneficial for older aged people. To sum it up, it is apparent that the system thus proposed is implementable on an intelligent devices or mobile devices. Hence the system is practically implementable.

REFERENCES

[1] Kuo-Hui Yeh "A Secure IoT-based Healthcare System with Body Sensor Networks ", IEEE Computer Society's IEEE Sensors Journal (2016).

[2] D. Malan, T. F. Jones, M. Welsh,S. Moulton, "CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care," Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004); Boston, MA, USA. 6–9 (2004).

[3] A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He , S. Lin, J. Stankovic, "ALARM-NET: Wireless Sensor Networks for Assisted-Living and Residential Monitoring," Department of Computer Science, University of Virginia; Charlottesville, VA, USA: (2006).

[4] J.W.P. Ng, B.P.L Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, G. Yang, "Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon)," Proceedings of 6th International Conference on Ubiquitous Computing (UbiComp'04); Nottingham (2004).

[5] R. Chakravorty, "A Programmable Service Architecture for Mobile Medical Care," Proceedings of 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06); Pisa, Italy. (2006).

[6] J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E, A. Terzis, G. M. Masson, "Median: Medical Emergency Detection in Sensor Networks," ACM Trans. Embed. Comput. Syst. vol. 10, pp. 1–29, (2010).