BSN – Care: An IoT - based Modern and Secure Healthcare System

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

P.G.Student, Department of Computer Engineering[1],
Head of Department, Department of Computer Engineering[2],

Amrutvahini College of Engineering, Sangamner, MH, India

Abstract:
Internet of Things (IoT) has emerged out of advances in information and communication technologies. The different medical fields like patient and healthcare management and real-time monitoring serve convenience to patients and physicians in modern environment. The modern technology of body sensor network (BSN) allows the monitoring of patients through the lightweight and tiny powered collection of sensors. BSN is regarded as a trending and hot technology in the field of healthcare using IoT. A system named BSN-Care which provides security to the healthcare system in IoT by using the BSN technology and with efficient accomplishment of all the requirements needed for security is proposed.

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

I. INTRODUCTION

Internet of Things has emerged out of advanced communication technologies. The application of IoT technologies brings a convenience. Body Sensor Networks is a core IoT technology in healthcare systems. A patient can be monitored using wireless sensors. IoT allows seamless interaction among different devices. A report recently published 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. Additionally, a research has indicated about the likelihood of the older aged people living independently is around 89 percent. Nevertheless, a research survey has found around 80 percent people of older age (i.e. older than 65) are likely to be affected by one or more fatal disease. It may result in difficulty in their self-care. Presently, one of the challenges is to provide a satisfactory and acceptable life to the older aged people socially. The growth in the communication and information technologies has been drastic over the years. It has enabled innovation in solutions of healthcare and tools that promise in addressing the challenges. In the 21st century prototypes of communication the most prominent is the Internet of Things. Due to their computing and communication capabilities all the daily life objects are becoming a part of the internet in the IoT environment, which is inclusive of transceivers and micro controllers for communicating digitally. The Internet as a concept is extended by IoT making it relatively widespread. Variety of devices including home appliances, medical sensors and monitoring cameras and so on can seamlessly interact through IoT.

II. LITERATURE SURVEY

Several projects and researches regarding wireless healthcare have been proposed recently. These aim at providing in-clinic, in-ambulatory, open environment, continuous patient monitoring. As the BSN technology has advanced in the healthcare environment and applications, patient monitoring has become more feasible. This section describes the relevant research projects that have been popular in healthcare applications using 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 amalgamates multiple sensor nodes that are low-powered, intelligent on and around the body of humans. The nodes detect not only the functions of the body but also the environmental and surrounding events. Potentially, the technology of healthcare and its future can be revolutionized greatly by the BSN technology. Basically, BSN comprises of in-body and on-body sensor networks. The sensors planted on the body establish a connection between the devices and the base station.

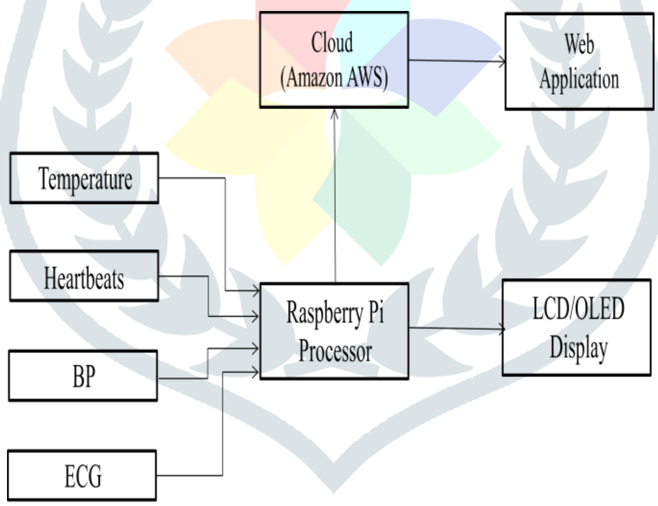

Figure 1 : Proposed system architecture

There are wearable sensors in the architecture of BSN-Care system (shown in Figure 1). The 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 biosensors, 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 collected through the sensors and communicated through MQTT protocol and published to the MQTT client. The Mosquitto broker communicates the messages among the clients. The collected data are then stored in the back-end client database for further analysis to predict the diseases on time and to provide timely medication. The end user dashboard can be prepared by subscribing the collected data from the MQTT client and this data is displayed in an interactive mode where everyone can understand the health status easily. The mail notification regarding the patient's current health can be sent to the doctor and the caretaker for further treatment. The dashboard can be viewed on a web server or Mobile API. The patient's location is monitored and this assures that the patient can be reached in case of any emergency situations. The patient's health status can be tracked through the dashboard regularly to improve the health conditions of the patients. Also a daily health tip can be provided based on the health conditions of the patients.

IV. ALGORITHMS DESIGN

The Message Queuing Telemetry Transport (MQTT) protocol is designed to operate in remote locations and on top of TCP/IP protocol in the Internet of Things. MQTT uses a little battery power and an efficient bandwidth. MQTT has these unique features over the other protocols:

1. MQTT being a lightweight protocol is easy to implement and is fast in transmitting data.
2. It makes a low usage of the network due to the minimized data packets.
3. Additionally, it makes low usage of power thus saving the connected device's battery.
4. Being a real-time protocol, MQTT best suits IoT applications.

The MQTT broker is a key entity of the protocol and can handle up to thousands of concurrently connected clients/subscribers.

1. **Subscribe**: The operation when a device wants to send the data to the broker.
2. **Publish**: The operation when a device wants to receive the data from the broker
3. **MQTT Broker**: The clients publish and subscribe to the topics and so the broker has to handle the actions of publish/subscribe to the respective topics.
4. **Topic**: The place where a device wants to put/retrieve a message to/from.

In the HTTP protocol a request/response mechanism is used for communication for every device that makes a connection to the IoT Agent. MQTT varies in a way that it uses publish-subscribe mechanism and is event-driven and pushes messages to clients.

MQTT Connection:

1. Any MQTT client and broker can establish the connection using MQTT protocol.
2. However, the connection amongst the clients cannot be established directly.
3. **It is required for the client to send a Connect message to the broker in order to initiate the connection with it.**
4. The response to the client's message is given by the broker by establishing the connection with it.
5. Upon the establishment of the connection, this connection is kept open by the broker waiting for a **Disconnect command** or unless the connection breaks for a reason.

Assume a device that has a temperature sensor on it and wants to send its readings to the broker. On the other side, a phone/desktop application will receive this temperature value. The two possibilities are thus:

- The device will defines the topic it wants to publish on, example: "temp". And then it publishes the message "temperature value".
- The phone/desktop application has subscribed to the topic "temp". So it receives the message that the device has published, that is the temperature value
.

The role of the broker is to take the message "temperature value" and deliver it to phone/desktop application.

Roles of the broker:

- It is the broker's responsibility to receive all the incoming messages, to analyze them, to filter them and then decide upon sending the messages to the subscribed clients as per their subscriptions of messages.
- The broker has to hold the information regarding the sessions of all the respective clients.
- Another prime responsibility of the broker is the authorization and authentication of its clients.
- As is the broker is generally expandable, the authorization, authentication and unification with the systems at the backend are facilitated.
- Handling the clients and communicating the messages amongst them keeps the broker always and frequently open to the internet.
- And so the broker has to be resistant to the failures, able to be monitored, unified with the backend systems and extensible.

V. RESULTS AND DISCUSSIONS

Experimental setup uses various datasets in order to analyze the accuracy of the stated algorithm. It improves the prediction of the possibility of the heart diseases. The performance of the algorithm can be analyzed on the basis of the measurement of the accuracy of predictions. Accuracy depicts the total number of success normal and success abnormal predictions for the specified dataset. Accuracy of each algorithm is specified in Table 1.

SML	Correctly classified instances	Wrongly classified instances
KNN	246	57
Logistic	254	49
Naïve Bayes	251	52
Random Forest	258	45

Table 1: Prediction Table

Accuracy = (SN+SA)/N, where N be the total number of records (i.e. 303).

The purpose of BSN-Care is to resolve several security issues in existing BSN based healthcare systems. It assures a feasible overhead for computation. We have compared the proposed healthcare system BSN-Care with the prevalent healthcare systems based on BSN technology and have manifested the benefits of the proposed system. Although all the predominant healthcare solutions based on BSN technology have addressed the requirements for privacy and security of the vulnerable data, only Alarm-net and Median i.e. the two of all these have incorporated any security. Table 2 represents the analysis of security of BSN-Care system in comparison to these existing systems.

In addition, Figure 3 represents the comparison between BSN-Care and Alarm-net system. It shows that it results in a less than half overhead of computation and the time of execution for BSN-Care, as compared to Alarm-net. It is of great use to the sensor devices. The privacy and security requirements in the applications related to healthcare that apply the BSN technology, are pivotal. As a result, it is evident that though the existing and approved prototypes based on BSN technology have the security issue acknowledged, these prototypes have substantially been unsuccessful to incorporate robust services for security needed to safeguard the privacy of the patients. Thus the proposed BSN-Care healthcare system is based on BSN technology and extends the areas of IoT. BSN-Care system can substantially consummate the varied requirements of security for the healthcare systems.

Table 2: Performance Analysis of Security Requirements

Security Requirements	Alarm-Net	Median	BSN-Care
Mutual Requirements	Yes	Yes	Yes
Anonymity	No	No	Yes
Secure Localization	No	No	Yes
Replay	No	No	No

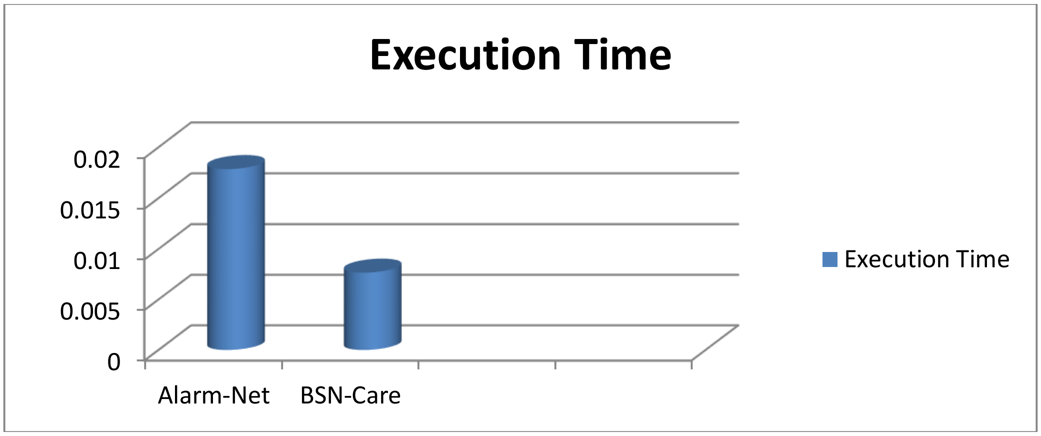

Figure 2: Performance of BSN-Care based on Execution Time

VI. CONCLUSION

BSN-Care can efficiently accomplish various security requirements of healthcare system. The authentication protocols guarantee network as well as data security. The cost of the system is user acceptable. It can be greatly convenient for aged people. In all, it is evident that the proposed system is suitable to be implemented on an intelligent or mobile device along with robust security mechanisms. Hence the system is practical.

VII. 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).