International Journal of Future Generation Communication and Networking
Vol.14, No. 1, (2021), pp. 4795 - 4798

Smart Iot Based Secure Framework For Healthcare Monitoring System Using Dynamic Rule Soft Signaling Method

Ms. T. Elavarasi, Dr. Senthil Kumar G,

[1]*Research scholar, Sri Ramakrishna college of arts and science (Autonomous), Coimbatore.*
[2]*Principal, Adithya College of Arts and Science, Coimbatore.*

ABSTRACT

Advancement in sensor technologies has resulted in the rapid evolution of the Internet of Things (IoT) applications for developing behavioral and physiological monitoring systems such as IoT-based student healthcare monitoring systems. Nowadays, a growing number of students living alone scattered over wide geographical areas, and tracking their health function status is necessary. In this work, an IoT-based healthcare monitoring model is proposed to continuously check vital signs and detect biological and behavioral changes via smart healthcare technologies. In this model, vital data are collected via IoT devices. Data analysis is carried out through the Dynamic Rule Soft Signaling (DRSS) method for detecting the probable risks of patient physiological and behavioral changes. The experimental results reveal that the proposed model meets the efficiency and proper accuracy for detecting the patient condition. This research work also mainly focuses on Electronic Health Records (EHRs) security requirements for storing, searching, accessing, sharing and auditing in Cloud Healthcare Monitoring System (CHMS) using Dynamic attribute-based encryption (DABE) system. After evaluating the proposed model, the Dynamic Rule Soft Signaling method and Dynamic attribute-based encryption (DABE) system have achieved the highest accuracy of 97%, which is a promising result for our purpose methods. The proposed methods' results outperformed decision tree, random forest, and multilayer perceptron neural network algorithms.

Problem Statement

i. The conventional physiological monitoring systems are too bulky to be used for wearable monitoring.
ii. There is a need for Remote Patient Monitoring to monitor the vital parameters in different environments such as hospitals, homes, and ambulatory setting
iii. Although there are many studies on medical management and the Internet of Things in the literature, there is no standardized protocol for sharing information across platforms.
iv. There is a need to support comprehensive monitoring, analysis, and storage and retrieving of data anywhere, anytime.
v. Existing systems reduce the scope of security options implemented in resource-limited environments

Objectives

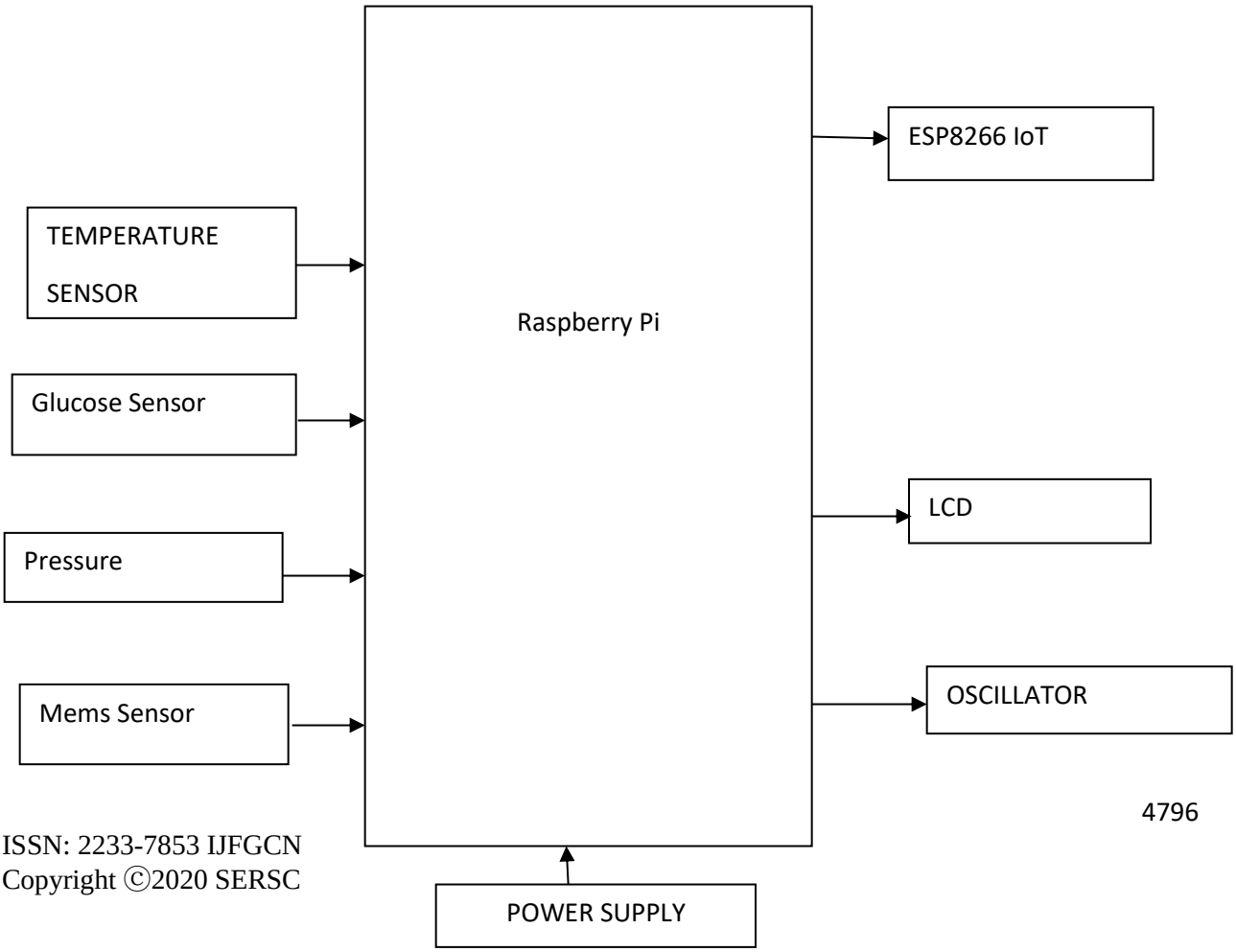
The primary objective of this research work is to design an efficient Healthcare monitoring system for the enablement of securely managing EHRs in the Cloud. The objectives of the research are enumerated as follows:

ISSN: 2233-7853 IJFGCN

i. To design a Healthcare monitoring system framework using an IoT platform and develop an IoT-based approach for disease diagnosis using the DRSS method.
ii. To identify various security issues and to design architecture to manage EHRs in Cloud using Searchable Symmetric Encryption.
iii. To improve the security for fine-grained access control of EHRs in the Cloud by removing key escrow and allowing immediate user revocation.
iv. To design a secure framework for ensuring EHRs integrity in the Cloud using fine-grained auditing.

Proposed System

In this proposed work, the vital parameters such as temperature, pressure, pulse oximeter and mems sensor readings are monitored using Raspberry pi. These sensor signals are sent to Raspberry pi via an amplifier circuit and signal conditioning unit (SCU). The signal level is low (gain), so the amplifier circuit can gain the signals and transmit the signals to the Raspberry pi. Here, patients' body temperature, heart rate, and pressure are measured using respective sensors. It can be monitored on the computer screen using Raspberry pi connected to a cloud database system and monitored worldwide using an internet source. The proposed method of patient monitoring system monitors patient's health parameters using Raspberry pi. After connecting the internet to the Raspberry pi, it is connected to a cloud database system that acts as a server. Then the server automatically sends data to the receiver system. Hence, it enables continuous monitoring of the patient's health parameters by the doctor. Any abrupt increase or decrease in these parameter values can be detected at the earliest, and hence necessary medications can be implemented by the doctor immediately.



ISSN: 2233-7853 IJFGCN

1. Raspberry pi is the controller board which is a heart-whole system using Dynamic Rule Soft Signaling
2. All the different analog sensors are connected to Raspberry pi through analog pins
3. Here the ESP8266 WiFi module connects the whole system to a WiFi network
4. Data from sensors are uploaded to the cloud with secure communication using the Dynamic attribute-based encryption method

Expected outcome

Communication among sensor nodes using the Internet is challenging since sensor nodes contain limited band width, memory, and small-sized batteries. The widely used microprocessor technique may overcome the issues of storage capacity. In this work, we have discussed some issues of PC, IOT& sensor network. To develop a new protocol in the sensor network, the specific application-oriented scenarios are of important consideration. Keeping this in mind, we have discussed some applications of a patient monitoring system.

REFERENCES

1. D. Malan, T. Fulford-Jones, M. Welsh, and S. Moulton, "Codeblue: An ad hoc sensor network infrastructure for emergency medical care," in International workshop on wearable and implantable body sensor networks, vol. 5. Boston, MA;, 2004.
2. J. W. Ng, B. P. Lo, O. Wells, M. Sloman, N. Peters, A. Darzi, C. Toumazou, and G.-Z. Yang, "Ubiquitous monitoring environment for wearable and implantable sensors (ubimon)," in International conference on ubiquitous computing (Ubicomp), 2004.
3. A. Wood, G. Virone, T. Doan, Q. Cao, L. Selavo, Y. Wu, L. Fang, Z. He, S. Lin, and J. Stankovic, "Alarm-net: Wireless sensor networks for assisted-living and residential monitoring," University of Virginia Computer Science Department Technical Report, vol. 2, p. 17, 2006.
4. J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao, W. Destler, L. Selavo, and R. P. Dutton, "Medisn: Medical emergency detection in sensor networks," ACM Transactions on Embedded Computing Systems (TECS), vol. 10, no. 1, p. 11, 2010.
5. S. C. Mukhopadhyay, "Wearable sensors for human activity monitoring: A review," IEEE Sensors Journal, vol. 15, no. 3, pp. 1321–1330, March, 2015.
6. P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," IEEE Sensors Journal, Vol. 16, no. 5, pp. 1368–1376, 2016.
7. H. Wang, J. Gong, Y. Zhuang, H. Shen, and J. Lach, "Healthedge: Task scheduling for edge computing with health emergency and human behavior consideration in smart homes," in 2017 IEEE International Conference on Big Data (Big Data). IEEE, 2017, pp. 1213–1222.
8. K.-H. Yeh, "A secure iot-based healthcare system with body sensor networks," IEEE Access, vol. 4, pp. 10 288–10 299, 2016.
9. X. T. Kong, H. Luo, G. Q. Huang, and X. Yang, "Industrial wearable system: the human-centric empowering technology in industry 4.0," Journal of Intelligent Manufacturing, pp. 1–17, 2018.

ISSN: 2233-7853 IJFGCN

10. Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," Information Sciences, vol. 479, pp. 567–592, 2019.
11. K. Sowjanya, M. Dasgupta, and S. Ray, "An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems," International Journal of Information Security, vol. 19, no. 1, pp. 129–146, 2020.
12. T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, "AGE: authentication in gadget-free healthcare environments," Information Technology and Management, pp. 1–20, 2019.
13. S. Binu, M. Misbahuddin, and J. Paulose, "A Signature-Based Mutual Authentication Protocol for Remote Health Monitoring," SN Computer Science, vol. 1, no. 1, p. 8, 2020.
14. M. Shuai, B. Liu, N. Yu, and L. Xiong, "Lightweight and Secure Three Factor Authentication Scheme for Remote Patient Monitoring Using on Body Wireless Networks," Security and Communication Networks, vol. 2019, 2019.
15. S. Sengupta, "A Secured Biometric-Based Authentication Scheme in IoT-Based Patient Monitoring System," in Emerging Technology in Modelling and Graphics. Springer, 2020, pp. 501–518.
16. N. Jalloul, F. Porée, G. Viardot, P. L'Hostis, and G. Carrault, "Activity Recognition Using Complex Network Analysis," IEEE journal of biomedical and health informatics, vol. 22, no. 4, pp. 989–1000, 2018.
17. K. Altun, B. Barshan, and O. TunÃ§el, "Comparative study on classifying human activities with miniature inertial and magnetic sensors," Pattern Recognition, vol. 43, no. 10, pp. 3605 – 3620, 2010.
18. F. Attal, S. Mohammed, M. Dedabrishvili, F. Chamroukhi, L. Oukhellou, and Y. Amirat, "Physical human activity recognition using wearable sensors," Sensors, vol. 15, no. 12, pp. 31 314–31 338, 2015.
19. A. Subasi, M. Radhwan, R. Kurdi, and K. Khateeb, "IoT based mobile healthcare system for human activity recognition," in 2018 15th Learning and Technology Conference (L&T). IEEE, 2018, pp. 29–34.
20. A. Mannini, S. Intille, M. Rosenberger, A. Sabatini, and W. Haskell, "Activity recognition using a single accelerometer placed at the wrist or ankle," Medicine and science in sports and exercise, vol. 45, no. 11, pp. 2193–2203, 2013.

ISSN: 2233-7853 IJFGCN