FOG BASED SECURITY PROTOCOL FOR NON-RESOURCE CONSTRAINED IOT DEVICES USING MOBILE NODES

Mrs.K.Balasaranya[1], K.sowmiya[2], K.Thaila[3], R.Thamizharasi[4]

[1]Assistant Professor, [2, 3, 4]Student (B.E), [1, 2, 3,4]CSE Department,
[1]R.M.D Engineering College, Kavaraipettai, Chennai-601 206, Tamil Nadu, India.

---***---

Abstract--The Monitoring Patient Health is evolving as a major problem in today's world. Patients are facing a problematic situation of unforeseen demise due to the specific reason of heart problems and attack which is because of nonexistence of good medical maintenance to patients at the needed time. This is for specially monitoring the old age patients and informing doctors and loved ones. So we using a project to dodge such sudden death rates by using Patient Health Monitoring that uses sensor technology. The main aim of project is to perform event based triggering to process the patient's real-time data and compute the data in patient's mobile and then data got uploaded to cloud. This system uses Temperature and heartbeat sensor for tracking patients health. This system propose the Secured OTP IoT Environment in Medical Field. The health related data get uploaded into Mobile node. The outcome of the project compute the data in patient's mobile and then data got uploaded to cloud. Thus, IoT based patient monitoring system effectively monitor patient's health status and save life on time.

Keywords: Secured OTP IoT, Mobile node, cloud, sensor.

I. INTRODUCTION

In the current trend Internet of Things (IoT) technology is more useful in healthcare in terms of mobile health and remote patient monitoring. IoT generates an unprecedented amount of data that can be processed using cloud computing. But for real-time remote health monitoring applications, the delay caused by transferring data to the cloud and back to the application is unacceptable. So when the health care IoT devices starts uploading current status of patient from smart home or hospital to the cloud continuously. The patient's mobile will be acting as Fog-node in which it collects the data and computes the received data and generates events for abnormal cases. When an event is triggered the cloud sends alert to doctor, ambulance and relatives based on the threshold of event occurred. All data transmission occurring in-between Cloud Server and Patient' Mobile is encrypted using One Time Pad security mechanism.

The problems existing in the current system are as follows:

- Due to continuous monitoring of IoT devices even the Fog Servers got accumulated with bulk of junk files.
- Processing the data in Edge Servers or Fog Servers takes very long time which makes slow alerts.

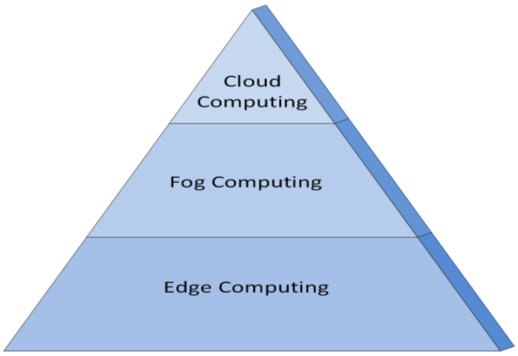

Fig.1.Fog Based IoT

II. EXISTING SYSTEM

IoT based remote monitoring systems have been suggested by various researchers due to their high efficiency in delivering intensive time-sensitive information to the clients. In existing system the IoT devices will keep observe the data from various resources and send data to the respective fognode or edge node for computation of health data. Then the computed values will be transferred to the cloud Server. Based on the abnormal condition the Cloud will send intimation to the clients.

III. PROPOSED SYSTEM

The Secured OTP IOT Environment in Medical Field is proposed. Here the patient's android mobile device will be acting as the edge server for doing computing with the receiving data from health monitoring devices. The health related data get uploaded into Mobile node. In Mobile Edge Layer, edge level computing is performed based on the threshold values the health status of respective patient is analyzed. If the status is getting abnormal then the Mobile Edge layer sends the health data with One time pad security to the Cloud. Then the emergency message will be sent to Hospital Ambulance, Doctor and relatives based on the type of event triggered. Mobile computing promotes high efficient output because maximum computation is done edge level which makes the cloud process as light weight. Thus it implements the computation in patient's mobile device with one-time-pad security.

IV. ARCHITECTURE

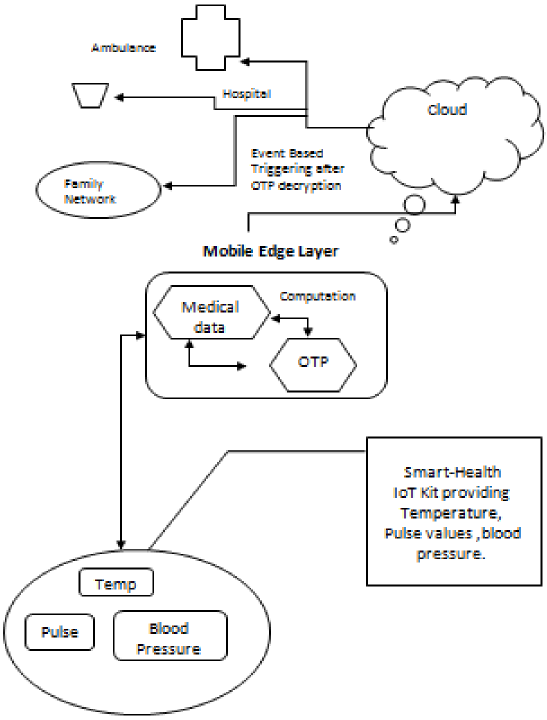
Ambulence
Hospital
Cloud
Event Based Triggering after OTP decryption
Family Network
Mobile Edge Layer
Medical data
Computation
OTP
Smart-Health IoT Kit providing Temperature, Pulse values ,blood pressure.
Temp
Pulse
Blood Pressure

Fig.2.Architecture

V. SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS

- Laptop-1
  - Hard Disk: 20GB & Above
  - RAM: 4GB & Above
  - Processor: Pentium IV & Above
- Mobile phone-2

Android: Jelly-Bean & Above

SOFTWARE REQUIREMENTS

- Windows 7 operating system and above
- JDK 1.8
- Android Studio

VI. MODULE DESCRIPTION

I. User Authentication in Web-portal

In this module we have developed a web portal – Hospital Web application. Using this application new patients has to register their details and the data will be stored in hospital Server. Likewise a hospital Admin sign-in will be there they can add new doctors and specific specialist to which the doctors belong to. All these information will be saved into hospital server's database.

II. Patient's Mobile Application and Appointment

The patient communicates with this system by registering his/her information at first instance by answering questions related to health history and personal details. After registration, a unique identification number is provided to the patient by the cloud server. To perform the classification, cloud layer provides the patient identification (PID) and attribute sets related to health history of the patients. The current application scenario works in event triggered mode. In this mode, the requisite real-time sampled data is stored at the mobile nodes. The mobile edge layer willconduct a data handling. Patients can request appointment to their respective Doctors from mobile application or web application.

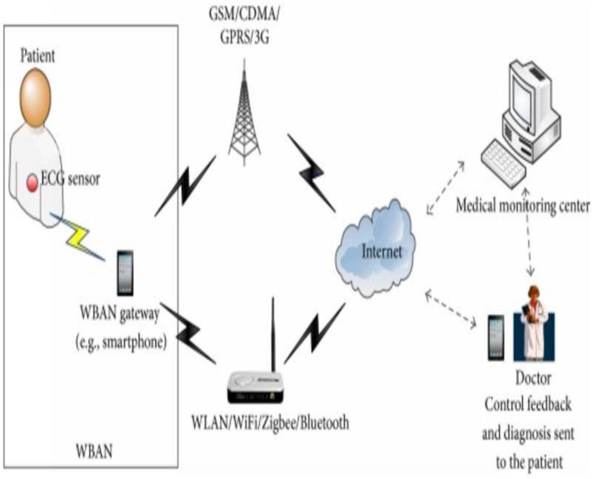
GSM/CDMA/ GPRS/3G
Patient
ECG sensor
Medical monitoring center
Internet
WBAN gateway (e.g., smartphone)
WLAN/WiFi/Zigbee/Bluetooth
WBAN
Doctor
Control feedback and diagnosis sent to the patient

Fig.3.Wireless Sensor Networks

III. Mobile Computing

The health data from various fog-nodes from respective areas will be processed in Mobile layer. Based on the previous health dataset the computation will be processed. Data from different categories will be analyzed here. Health related data from previous history got collected from the Health dataset, Environment related data like air quality, noise level around the place where patient is, Behavior related data like whether the patient is having fits, vomiting, hyper tension, fainting etc. These kinds of data get analyzed in this layer. After computing , the end result will be sent to the one-time-pad.

IV. Event Based Triggering

When the mobile device performs computation periodically when the values got reached above the threshold value then it will detect that patient is in emergency state and has abnormal condition. So spontaneously the mobile node will send the abnormal data to the Cloud in encrypted format and here the Event is triggered by the cloud server. The Emergency alert to the Doctors, medical team, ambulance, relatives, etc . Thus the alert will be sent to respective mobile users.

VII. RESULT

We propose the Secured OTP IOT Environment in Medical Field. Here the patient's android mobile device will be acting as the edge server for doing computing with the receiving data from health monitoring devices. The health related data get uploaded into Mobile node. In Mobile Edge Layer, edge level computing is performed based on the threshold values the health status of respective patient is analyzed. If the status is getting abnormal then the Mobile Edge layer sends the health data with One time pad security to the Cloud. Then the emergency message will be sent to Hospital Ambulance, Doctor and relatives based on the type of event triggered. Mobile computing promotes high efficient output because maximum computation is done edge level which makes the cloud process as light weight. We going to implement the computation in patient's mobile device with one-time-pad security.

VIII. CONCLUSION

Thus to perform event based triggering to process the patient's real-time data and compute the data in patient's mobile and then data got uploaded to cloud.

References

[1] M. Chiang and T. Zhang, "Fog and IoT: An overview of research opportunities," IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854– 864, 2016.

[2] H. Farhangi, "The path of the smart grid," IEEE power and energy magazine, vol. 8, no. 1, 2010.

[3] F. Computing, "the internet of things: Extend the cloud to where the things are," Cisco White Paper, 2015.

[4] X. Lin and X. Li, "Achieving efficient cooperative message authentication in vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 62, no. 7, pp. 3339–3348, 2013.

[5] C. C. Datasheet, "2.4 GHz IEEE 802.15. 4," ZigBee-Ready RF Transceiver (Rev. B), 2012.

[6] K. Boakye-Boateng, E. Kuada, and E. Antwi-Boasiako, "Efficient encryption protocol for wireless sensor networks using one-time pads," in Electrotechnical Conference (MELECON), 2016 18th Mediterranean.IEEE, 2016, pp. 1–6.

[7] J. Zhu, D. S. Chan, M. S. Prabhu, P. Natarajan, H.Hu, and F.Bonomi, "Improving web sites performance using edge servers in fog computing architecture," in *2013 IEEE Seventh International Symposium on Service-Oriented System Engineering*, pp. 320–323, Redwood City, USA, March 2013.

[8] Y. Chen, W. Shen, H. Huo, and Y. Xu, "A smart gateway for health care system using wireless sensor network," in *2010* Fourth International Conference on Sensor Technologies andApplications, pp. 545–550, Venice, Italy, July 2010.

[9] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: a programming model for large-scale applications on the internet of things," in Proceedings of the Second ACM SIGCOMM Workshop on Mobile Cloud Computing, pp. 15–20, Hong Kong, China, August 2013.

[10] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[11] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: a secure sensor network communication architecture," in Information Processing in Sensor Networks, 2007. IPSN 2007. 6th International Symposium on. IEEE, 2007, pp. 479–488.

[12] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[13] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, pp. 739–763, 2004.

[14]C. Karlof, N. Sastry, and D. Wagner, "Tinysec: a link layer security architecture for wireless sensor networks," in Proceedings of the 2nd international conference on Embedded networked sensor systems. ACM, 2004, pp. 162–175.

[15] J. Daemen and V. Rijmen, The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[16] A. Moh'd, N. Aslam, W. Robertson, and W. Phillips, "C-sec: Energy efficient link layer encryption protocol for wireless sensor networks," Conference (CCNC), 2012 IEEE. IEEE, 2012, pp. 219–223.

AUTHORS PROFILE

K.Sowmiya Fourth Year Student currently pursuing B.E(CSE) in R.M.D Engineering college, Chennai, Tamil Nadu, India. Her areas of interest include web development, data structures and object oriented analysis and design.

K.Thaila Fourth Year Student currently pursuing B.E(CSE) in R.M.D Engineering college, Chennai, Tamil Nadu, India. Her areas of interest include Data Structures and Algorithms, Software Programming and object oriented analysis and design.

R.Thamizharasi Fourth Year Student currently pursuing B.E(CSE) in R.M.D Engineering college, Chennai, Tamil Nadu, India. Her areas of interest include Programming and Data Structures, Database Management System, Full stack web development.

Mrs.K.Balasaranya, B.Tech, M.E, M.B.A, is working as an Assistant Professor in R.M.D Engineering college, Chennai, Tamil Nadu. She has 10 years of experience in teaching Computer Science. Her fields of interest include Machine Learning and Data Mining.