Intelligent Systems and Computer Technology
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC200119

Healthcare Monitoring with Fog-Based IoT Kit and One Time Pad Encryption

Sangeetha M[a,1], ILakkiya S [b], Gandham Mahima[b], Ezhiloviya Chelvan [b]
[a]*Associate Professor, Dept of CSE, Panimalar Engineering College, Chennai*
[b] *UG Scholar, Dept of CSE, Panimalar Engineering College, Chennai*

Abstract. In the current trend, Internet of Things (IoT) technology is more useful in healthcare in terms of mobile health and remote patient monitoring. IoT produces enormous data to be processed in cloud. In practice, the latency caused by cloud for processing the data leads to unacceptable losses. As an alternative method, we have proposed a system to reduce the latency caused. The health care IoT devices start emitting the data relevant to a patient. The data are then uploaded as current status of a patient from smart home or hospital to the cloud continuously. The mobile of each patient 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 Mobile of each patient is encrypted using One Time Pad security mechanism. The proposed encryption mechanism is a lightweight encryption compatible with IoT based system. Since it has an encryption that is yet to be cracked, we can ensure secure transmission of patient records with a higher performance than which was achieved by cloud computing.

Keywords. Fog-node, One Time Pad, encryption, Cloud server, Internet of Things (IoT), latency.

1. Introduction

The technology that progresses each day at the speed of lightning generates enough data to fill up all the storage devices in the world. Sometimes, this huge amount of data leads to new problems that may arise in critical situations. In such situations, faster processing of data and faster reactions are required. Taking into consideration one such critical aspect may arise in a medical field.

IoT (Internet of Things) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network".

An IoT system for Healthcare monitoring of patients has been proposed. This system monitors a patient's heart beat, blood pressure and temperature through sensors. All data from the IoT kit is sent to a patient's mobile phone which is forwarded to the hospital cloud server. The continuous stream of data to the cloud server makes performance of server slow. So, we propose to introduce Fog computing.

Fog computing or fog networking, also known as fogging, is an architecture that uses edge devices to carry out a substantial amount of computation, storage, communication locally and routed over the internet backbone".

[1]Sangeetha.M, Associate Professor, Dept of CSE, Panimalar Engineering College, Chennai;
E.mail:id :sangeetharemi@yahoo.co.in

2. Literature Review

Kwasi Boakye-Boateng *et* al[1] has proposed an Encryption Protocol for Wireless Devices using One Time Pad Encryption. In this paper, an encryption protocol is applied to wireless transmission devices like mobile phones which acts as Fog-node for secure data transmission. The paper is general and common to many applicationsMedicine, Telecommunication, Big Data Analysis and many more. Dharmendra Singh Rajput, Rakesh Gour [2] has proposed an IoT framework for healthcare monitoring system. The system measures heartbeat, temperature and other factors and the data is sent to the cloud for processing. There is no encryption done here and the data is processed in the cloud only. G. Meera Gandhi *et* al[3] has proposed a security framework for cloud based health monitoring system. In this paper the security algorithm used is Rabin's algorithm and they have proposed a system to monitor patient's health using IoT. T. Gebremichael *et* al[4] has proposed a group key establishment scheme using One Time Pad encryption in IoT devices. It uses symmetric key encryption and is based on perfect secrecy of One Time Pad. The disadvantage is that it is difficult to implement in real time hardware devices. Gopika Premsankar *et* al[5] has proposed a Edge Computing for IoT as a Case study. The paper explains the necessity of Edge computing to avoid the latency that arises in cloud computations Negash B. *et* al[6] has proposed has proposed a leveraging fog computing technique for healthcare IoT. This paper is about smart wearable IoT devices to monitor the physiological signs of the patient that are connected to the internet using fog computing layer. Here use of fog computing layer to implement smart e-health gateway connecting both home and hospitals is explained. Since fog computing layer is closer to sensor network, data analytics and adaptive services are possible in this technique. Parasuraman, Shalini, and Arun Kumar Sangaiah [7] have proposed a fog-driven healthcare framework for security analysis. In this paper the e-health sensitive data stored in cloud are secured from data thefts using advanced and decentralized fog based healthcare framework. Its advantage over RSA and ECC algorithms is that this system provides better performance and higher security.

3. Proposed System

The system proposed is mainly used for secure transmission of sensitive data and to prevent the latency occurrence in computation of the values from sensors.Since, this is related to the human health more care should be taken to avoid latency especially in times of emergency. The system consists of four modules each detailed in the upcoming paragraphs.

3.1. User Authentication

In this module there exists a Hospital 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 specialization to which the doctors belong to. All this information will be saved into hospital server's database.

3.2. Patient's Mobile Application

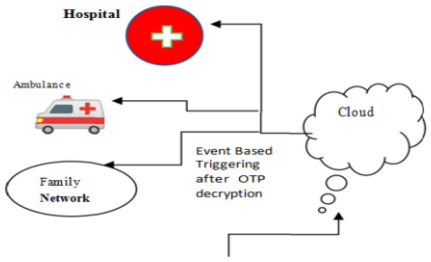
The patient communicates [12] with the server by registering his/her information at first instance by answering questions related to health history and personal details. After registration, a unique identification number is provided to the patient by the cloud server. To perform the classification, cloud layer provides the patient identification (PID) and attribute sets related to health history of the patients. The mobile edge layer will conduct a data handling. Patients can request appointment to their respective Doctors from mobile application.

3.3. Mobile Edge 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.Health related data from previous history is collected from the Health dataset, 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 security mechanism.

3.4. Event Based Triggering

The mobile device performs computation periodically. When the values cross the threshold value, 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 will be sent to the Doctors, medical team, ambulance, relatives, and other concerned people.The system is thus detailed with the modules in it. The IoT medical kit consists of Temperature sensor, Pulse rate and Blood Pressure sensors. It provides the values to the respective mobile phones of patients where they are computed, encrypted with One Time Pad encryption and sent to the cloud server.The cloud server decrypts the data it receives and according to the nature of emergency alerts the respective doctor, friends, relatives, ambulances and other concerned members.



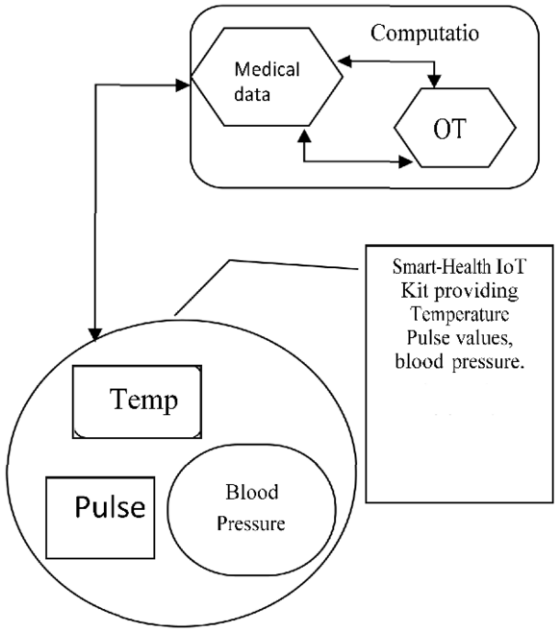


Figure 1. System Architecture

4. Methodology

The system uses Fog server extended to the edge of the network to reduce the latency. It uses One Time Pad encryption to ensure secure transmission. There are many security issues like trust, privacy, End user's privacy and many more faced by Fog computing [8]. One Time Pad (OTP) algorithm is an encryption algorithm invented by Frank Miller [9]. This encryption algorithm uses a Random Number Generator (RNG). The Random Number Generator is used to generate a number randomly which is taken as the key for the data to be encrypted. Since the key is generated randomly the algorithm is not easily traceable. This algorithm is chosen to be used because other encryption protocols like C- Sec, Zigbee and TinySec leads to energy and packet loss. But this algorithm results in zero packet loss [10].One Time Pad algorithm takes a data to be encoded which is the Plain text. It is converted to binary form. A key is generated using Random Number Generator which is also converted to binary form. An XOR operation is performed with the plain text and key which gives a binary number. The number is converted to decimal which gives the cipher text.

Key : 23
Plaintext : C
ASCII value of C : 67
Binary value of 67 : 0110 0111
Binary value of key : 0010 0011

XOR Operation

0110 0111

0010 0011

0100 0100 ⟹ 44

Cipher text: 44

The encrypted data is sent to the cloud from the mobile phone. The cloud server decrypts the data sent from the mobile phone and acts according to the nature of the data it receives.

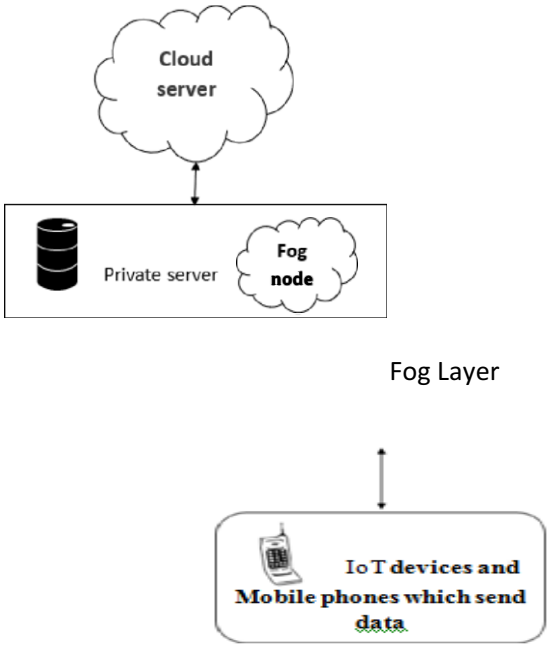
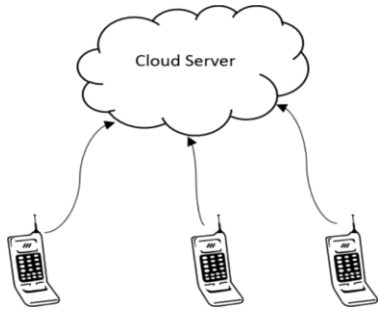


Figure 2. Traditional Fog Computing Architecture

Another methodology used is Mobile Edge Computing. Mobile Computing[11] is the process where mobile acts a computation device and sends the result to other sensors or devices. So, each mobile phone acts as a computation device and saves bandwidth and latency processing time.The mobile phones act as Fog nodes or secondary computation servers at the edge of network. Hence, it implements Fog computing and Mobile Edge Computing. As the data is sent from the mobile to the cloud, it does not cause overheating of mobile phones. Because data is not transmitted continuously. It is event triggered and only acts when necessary. Data is sent from sensors to mobile and then mobile to cloud through Bluetooth and Internet.



5. Results and Analysis

The One Time Pad algorithm is a lightweight process for IoT system. It also is yet to be cracked. The mobile phone is used as a Fog node. It reduces cost of Fog computing and mobile phones are commonly used now a days. Also, Mobile Edge Computing is implemented. Thus, an economically feasible system is developed for a Healthcare Monitoring System using an IoT kit.

6. Conclusions

The paper proposes the introduction of One Time Pad encryption in Fog based IoT healthcare monitoring kit. Also, the system helps to reduce the latency, save bandwidth and ensures secure transmission of sensitive data. It encrypts patient's details and their health-related data and makes certain that timely help is guaranteed in emergency situations.

References

[1] K. Boakye-Boateng, E. Kuada, E. Antwi-Boasiako, E. Djaba,.Encryption protocol for resource-constrained devices in fog-based IoT using one-time pads. IEEE Internet Things J., Apr. 2019. vol. 6, no. 2, p. 3925-3933.

[2] Dharmendra Singh Rajput, Rakesh Gour.An IoT Framework for Healthcare Monitoring Systems.International Journal of Computer Science and Information Security IJCSIS May 2016.Vol. 14, No. 5.

[3] G. Meera Gandhi, J. John Jasper and Emmanuel Andrew.Security Framework for Cloud Based Medical Monitoring System.Asian Journal of Engineering and Applied Technology ISSN: 2249- 068X Vol. 6 No. 1.2017. pp.23-28.

[4] G. Premsankar, M. Di Francesco, T. Taleb .Edge computing for the Internet of Things: A case study.IEEE Internet Things J., Apr. 2018.vol. 5, no. 2, pp. 1275-1284.

[5] B. Negash, T.N.Gia, A. Anzanpour, I. Azimi, M.Jiang, T.Westerlund, A.M.Rahmani, P.Liljeberg, H.Tenhunen, Leveraging Fog Computing for Healthcare IoT, Cham: Springer International Publishing, pp. 145-169, 2018.

[6] Parasuraman, Shalini, and Arun Kumar Sangaiah .Fog-driven Healthcare Framework for Security Analysis . In Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications, Academic press, 2018.
p. 253-270.

[7] J.Ni, K.Zhang, X.Lin, X.S.Shen .Securing fog computing for Internet of Things applications: Challenges and solutions . IEEE Commun. Surveys Tuts., 2018.Vol. 20, no.1, pp. 601-628, 1st Quart.

[8] Steven M. Bellovin 2011 Frank Miller: Inventor of the One-Time Pad, Cryptologia, 35:3, 203-222,

DOI: 10.1080/01611194.2011.583711.

[9] K. Boakye-Boateng, E. Kuada and E. Antwi-Boasiako.Efficient encryption protocol for wireless sensor networks using one-time pads. 2016 18th Mediterranean Electro-technical Conference MELECON. Lemesos, 2016. p. 1-6.

[10] Ejaz Ahmed, Mubashir Husain Rehmani, "Mobile Edge Computing: Opportunities, Solutions, and Challenges", *Article in* Future Generation Computer Systems · September 2016.

[11] T.Ramya, G.Pratheeksha, S.Malathi .Personalized authentication procedure for restricted web service access in mobile phones.Fifth IEEE International Conference on the Applications of Digital Information and Web Technologies ICADIWT.2014.p.69-74.

[12] S.Hema Kumar, J.Uday Kiran, V.D.Ambeth Kumar, G.Saranya, Ramalakshmi V, "Effective Online Medical Appointment System", International Journal of Scientific & Technology Research, Volume 8, Issue 09, September 2019, Pages 803 – 805.