SECURITY IN FOG IOT-BASED HEALTHCARE FRAMEWORK FOR HYPERTENSION

S. Farisha, Easwari *Engineering College, Chennai, Tamil Nadu*
V.Mercy Rajaselvi, Easwari *Engineering College, Chennai, Tamil Nadu*
Dr.G.S.Anandhamala*, Easwari Engineering College, Chennai, Tamil Nadu*
P.Hari Kumar*, Easwari Engineering College, Chennai, Tamil Nadu*

Abstract
A definitive issue always occuring in cloud is security. To vanquish the issues or issues of security, another strategy called Fog processing is introduced. The health information is taken from different sensors and fog framework is utilized in dissecting the hypertensive stage. The security of the patient's health information is significant. As the fog has many security issues, the strategy of encryption uses AES computation used here to secure the information of the fog. AES figuring is the most safeguarded about method of encryption for security. The datasets are examined and inspected encryption technique over those datasets. Further, execution of encryption is overviewed over picked datasets for precision if the whole information is sufficiently blended and unscrambled close by the time, User load, Response time, Memory Utilization over document size.

Index Terms—*AES computation, fog processing, memory utilisation, hypertensive stage, encryption.*

I.INTRODUCTION

Hypertension frequency in our country is high, but the individuals who really care about this disease and get treated are very low. Hypertension which is also known as high blood pressure is a silent killer as it can cause serious trouble if left untreated for long time[1]. Hypertension is also a risk factor for cardiovascular disease[4] that causes death.

The preventive measures have to be taken to avoid such risks that leads us to death. The proposed system proposes several modules that is used to identify the pre hypertension stages in human being to avoid hypertension attack in future and also secures the data. The individual blood pressure data is collected through the sensors and sent to the fog system. This data which is sent to the fog system is protected by the proposed system. Many hypertension techniques which have been proposed earlier had some drawbacks related to accuracy and security. With this proposed system the accuracy and security issues can be solved because the modules proposed in this system deeply analyze an individual's pulse rate and protect the persons health data[3]. The sensor to cloud architecture is not very suitable for the healthcare applications.

Many doctors would not wish to store patient data in the cloud because delay of retrieving the data in case of network failure[15]. If only the cloud is used, it would cause delay while transferring of data from the sensors to the cloud and the data from cloud to the hospitals or their concerned family members. So the fog helps to divide the system work and helps in generating the alert quickly to the doctors and their concerned family members. Always the medical data is very confidential so doctors will not like to share the data with anyone, therefore the security is very necessary for the health data. The cyber security evaluation allows to secure the health data collected by the sensor.

II.RELATED WORK

A. KEY OBJECTIVES ABOUT THE HEALTH CARE SYSTEM:

(1) better medicine the executives
(2) decreased duplication of demonstrative testing, imaging, and history taking
(3) Improved clinical dynamic.
(4) Better reachable of health services to the remote place patients.

B. SECURITY IN FOG COMPUTING THROUGH ENCRYPTION:

Once Data Encryption standard (DES)[2] was general algorithm that was used by most people for encryption process. The key size of DES is 56 bits whereas the square size of the key is 64 bits. For some applications, considering this algorithm became much uncertain or we can say it was not suitable for some applications. This is a direct result of its key size which is 56 bits and this could be brute forced. Two of the organizations together before, broke the DES algorithm key in 22 hours and 12 minutes. By this we can analyse that the DES algorithm is powerless and easily breakable. Therefore, In this way AES encryption method was created for analysis and protect IOT information.

To conquer the above issue, referenced Advanced Encryption Standard (AES) is considered as progressively effective. AES is seen as the most incomparable and secure standard for encryption of electronic information collected by sensors. AES is viewed as successor of the DES. The AES encryption algorithm uses standard symmetric key encryption for many of the US government associations because of its efficiency. AES accepts the key size of 128, 192, 256 bits of size. While today 128 is considered as unbreakable. And also at that time there were many organisations that tried to break the key ,yet it was rarely done. On looking at all the accessible encryption algorithms, AES would be the better and most secure type of algorithm that could provide security in the fog system. As when all the encryption procedure are considered, AES can be observed as increasingly reasonable and versatile for nature of fog. Henceforth this paper compiles applying of AES algorithm for security of the information in fog processing through an edge gadget of mobile.

C. FOG COMPUTING:

A system was proposed was proposed to recognize the hypertension in pregnancy time. This framework distinguishes a hypertension issue in pregnant woman before the hypertension assault. This grouping strategy assists to identify the risks, dangers, analyze and can diminish maternal[12] and fetal mortality. The home self-blood pressure monitoring was proposed to make blood pressure checking accessible at home. The individuals can check their blood pressure at home and monitor it. The Self-blood-pressure monitoring (SBPM) is the best decision for long-term follow-up. SBPM is more powerful than BP estimated by an expert

(PBPM) in that it has a more prominent prescient significance connects better with the end organ harm. The people who are disabled physically and living alone or distant from human services administrations need to deal with their wellbeing without anyone else. This framework permits to deal with their wellbeing even at remote spots.

IoT-Fog based human services framework is proposed for continuous observing and examination of BP measurements to identify hypertensive clients[8]. The proposed framework at first identifies the phase of hypertension based on client's wellbeing parameters gathered utilizing IoT sensors at fog layer. After recognizing the hypertensive stage, artificial neural system is utilized for predicting the hazard level of hypertension assault in clients at remote sites.

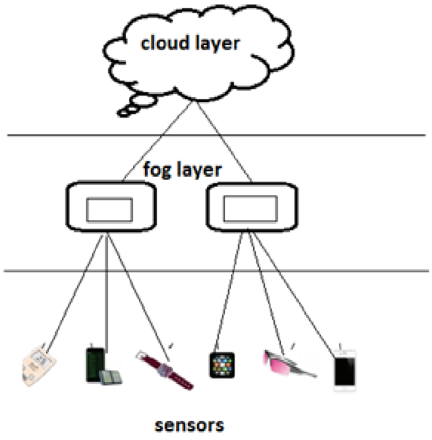

Figure1.Layers in IoT

III. PROBLEM DEFINITION

Security[9] is becoming the major fear these days because there are many sensitive data everywhere. This can be any company details, or medical information in hospitals or even it could be national secret. All the data must be secured and should make sure that it has all necessary methods in it, which makes an attacker difficult to crack the key.The paper primarily concentrates on security and privacy of data. In the system, though secured data is sent to the fog from cloud, guessing the security threat in the fog is a difficult thing, so its better to add a second layer of security within the level of fog.

IV.PROPOSED SYSTEM

The four modules have been created for collecting the data, securing the data and analysing the data.

A. IoT user system

The IoT system can be considered as the first module in the system to obtain the health data from the user module.This user system get the health details from the user and monitors the activities of the user. User subsystem comprises of various IoT devices and sensors to capture hypertension activities that causes hypertension.While obtaining the health details ,Health attributes such as SBP, DBP[4] plays main role.Here the SBP and DBP of a person is analysed to predict the persons hypertension stage.The patient s BP rate is collected through the various input sensor devices. In the existing system, the health data[13] are collected from various wireless sensor devices. Therefore, enormous amount of data is produced by the sensors which is then sent to fog layer for processing and analysis[6]. The utilization of keen gadgets has serendipitously been practiced in medicinal services. Nowadays, it is typical to discover a scope of medicinal services contraptions that can be utilized by patients at home or even worn by them. The contraptions for the most part incorporate sensors.

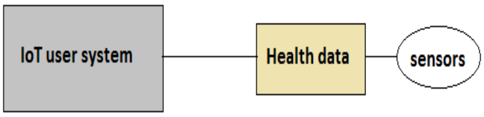

Figure2.Iot user system

B.FOG SYSTEM

This layer performs information examination and collection of the information. The information and data gathered by the edge gadgets are examined in this layer. This layer carries on as the worker. Gigantic measures of constant information from sensors are sent to this layer[5]. The Health fog subsystem is the center layer between IoT sensors and distributed computing. It is utilized for continuous handling and examining of collected information from IoT based sensors. It quickly sends constant notifications or alarms[11] to user about the current stage of hypertension to prevent the chronic condition in an early stage[7]. This subsystem is additionally associated with a cloud framework for putting away, examining results and accumulating clinical record of every client.

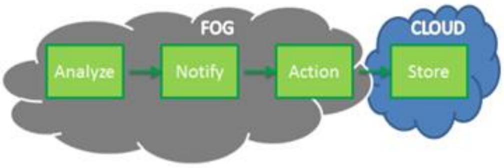

Figure3. Fog system

C.CLOUD SYSTEM

Cloud Subsystem is responsible for storing intermediate and final results of user health status. It consists of huge amount of storage to store analysis results, compiled medical information of each user and share among authorized medical staff, users, pharmacies, hospitals and healthcare professionals. Government aided healthcare centers can also upload data as well as any information regarding first aid, free camps, etc. User and authorized entities can access medical records anytime from any place. Temporal data granulation component in health fog system sends data granulation information to a cloud system for permanent storage so that it can be accessed by any other component of fog system in anytime for further analysis. Similarly, alert messages[14] regarding the current status of hypertension are also stored on cloud storage for further analysis by experts to take immediate action and provide precautions in case of emergency.

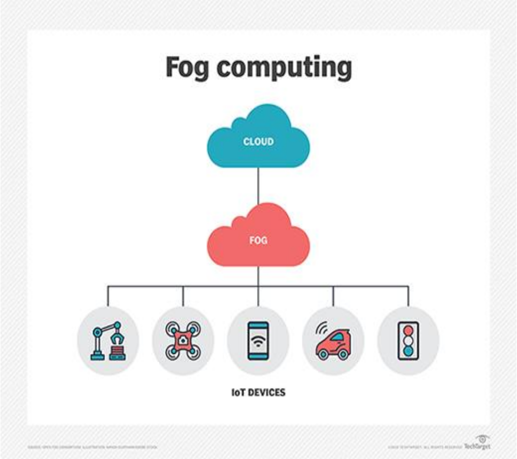

Figure 4. Fog system with cloud

D.AES ALGORITHM

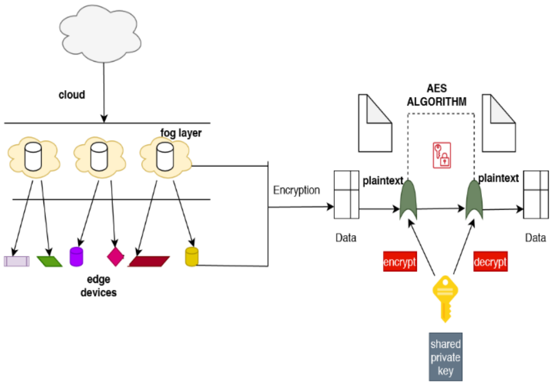

Figure 5. Working of AES algorithm in fog system.

AES algorithm[2] is most widely used algorithm for encrypting and decrypting sensitive information like medical information. AES algorithm is considered to be an advanced of DES algorithm. The AES algorithm uses symmetric key block cipher means that the same key is used for encryption and decryption. AES accepts of the key size of 128, 192, 256 bits of size. Whereas 128 is already considered to be unbreakable. Here the 128 bits of data of plaintext where the 128 bit key works on it and the output is regarded as 128 bit cipher key. The key depends on the number of rounds.

TABLE I.THE RELATIONSHIP BETWEEN THE NUMBER OF ROUNDS AND KEYS

NO.OF KEY USED	ROUNDS
10	128
12	192
14	256

The encryption of AES can be divided into three modules namely the initial round, the main rounds, and the final round. All of the modules[10] use the same sub-operations in different combinations as follows:

Initial Round: AddRoundKey

Main Rounds: SubBytes ShiftRows MixColumns AddRoundKey

Final Round: SubBytes ShiftRows AddRoundKey

AddRoundKey: The AddRoundKey activity is the main period of AES encryption that straightforwardly works on the AES round key: In this activity, the contribution to the round is selective or with the round key.

SubBytes: The SubBytes period of AES includes parting the contribution to bytes and going each through a Substitution Box or S-Box. In contrast to DES, AES utilizes a similar S-Box for all bytes.

ShiftRows: In the ShiftRows period of AES, each line of the 128-bits inner condition of the code is moved. The columns in this stage allude to the standard portrayal of the inward state in AES, which is a 4x4 framework where every cell contains a byte. Bytes of the inside state are put in the network across lines from left to right and down segments. In the ShiftRows activity, every one of these columns is moved to one side by a set sum: their line number beginning with zero. The top column isn't moved in any way, the following line is moved by one, etc.

MixColumns: Like the ShiftRows period of AES, the MixColumns stage gives dissemination by blending the contribution around. Dissimilar to ShiftRows, MixColumns performs activities parting the lattice by segments rather than columns.

Decryption in AES: To decrypt an AES-scrambled ciphertext, it is important to fix each phase of the encryption activity in the converse request in which they were applied. The three phase of decryption are as per the following:

Inverse Final Round: AddRoundKey ShiftRows SubBytes

Inverse Main Round: AddRoundKey MixColumns ShiftRows SubBytes

Inverse Initial Round: AddRoundKey
Just the AddRoundKey activity is its own converse (since it is an elite or). To fix AddRoundKey, it is just important to extend the whole AES key timetable (indistinguishably from encryption) and afterward utilize the proper key in the restrictive or. The other three activities require an opposite activity to be characterized and utilized. The principal activity to be fixed is ShiftRows. The Inverse ShiftRows activity is indistinguishable from the ShiftRows activity with the exception of that pivots are made to one side rather than to one side. The following activity to be fixed is the SubBytes operation.It is perused indistinguishably from the S-Box matrix.The last backwards activity to characterize is MixColumns. Like MixColumns, Inverse MixColumns can be characterized as the lattice increase. AES ciphertexts are decoded by this request for activities clarified previously. The accompanying chart clarifies about how the tasks all together are performed to scramble and unscramble the information.

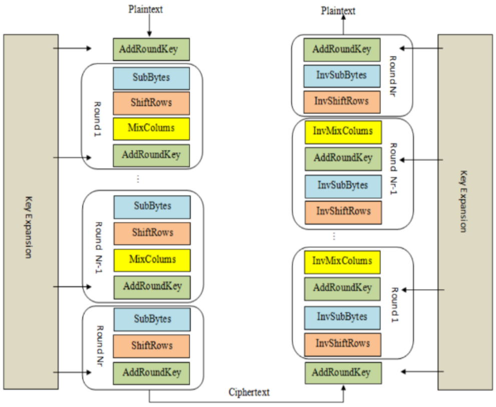

Figure 6. AES algorithm

VI. CONCLUSION

Fog computing is considered to be one of the major part in the computing world, and as there are millions of devices connected and as IOT would be a major part of it, there may be a lot of issues on security. So our research here considered data security as the key factor and implemented Advanced Encryption Standard (AES) in the fog computing. This adds a second layer of security for data and makes difficult for intruder to sense the data.

Different datasets are choosen and applied the AES algorithm for encryption and decryption for each of the dataset. Analysing of different metrics is done so as to evaluate the adaptability of AES in second layer of cloud system of fog. As our future work, we would like to implement AES with key size of 512 bytes in fog. So that security becomes more stronger

REFERENCES

[1]Anand Paul , Hameed Pinjari, Won-Hwa Hong , Hyun Cheol Seo and Seungmin Rho(2018), 'Fog Computing-Based IoT for Health Monitoring System', Journal of Sensors, Vol.10,pp.386-470.

[2]Akhilesh Vishwanath, Ramya Peruri(2016), 'Security in Fog Computing through Encryption' , International journal of Information Technology and Computer Science, volno.5, pp.28-36.

[3]A. Alavudeen basha and S.Vivekanandan (2019), 'Enhanced optimal insulin regulation in post-operative diabetic patients: an adaptive cascade control compensation-based approach with diabetic and hypertension', IEEE internet of things journal , vol.7, no.2, pp. 90973 - 90981.

[4]M. Anna Latha and N.Christy Evangeline (2018) ,'Colour Image Segmentation of Fundus Blood Vessels for the Detection of Hypertensive Retinopathy', International journal of Biosignals, Images and Instrumentation,vol.52, no.3, pp.22-28.

[5].F.Bonomi, R.J. Milito and S. Addepalli (2012) ,'Fog computing and its role in the Internet of Things: Characterization of fog computing', IEEE journal of Mobile Cloud Computing, vol.25, no.3, pp.13–15.

[6]A.V.Dastjerdi and R. Buyya (2016), 'Fog computing: helping the Internet of Things realize its potential', IEEE Internet of thing journal, vol. 49, no. 8, pp. 112 – 116.

[7]Frank alexander kraemer, Anders eivind braten, Nattachart tamkittikhun, and david palma, (2017)'Fog Computing in Healthcare—A Review and Discussion', IEEE ACCESS , vol.5, no.3, pp.25-32.

[8].M.Hamed Orojloo1 and Mohammad Abdollahi Azgomi (2018),'Modelling and evaluation of the security of cyber-physical systems using Stochastic Petrinets', IET journal of engineering and technology,vol.25, no.4, pp. 23-36.

[9]Lu-xing yang, pengdeng li and Xiaofan yang and Yuan yan tang(2017)'Security Evaluation of the Cyber Networks Under Advanced Persistent Threats', journal of Computer and Information Science, vol.23,no.3,pp.112-119.

[10]M. Sri Lakshmi, Dr. B. Lalitha, (2017), 'Enhancing the Security for Clinical Document Architecture Generating System using AES Algorithm with Artificial Neural Network', International Research Journal of Engineering and Technology Vol.4 no. 08, pp.239-280.

[11]Mario Pascual Carrasco, Pilar G. Sagredo ,(2008) 'Impact of Patient–General Practitioner Short-Messages-Based Interaction on the Control of Hypertension in a Follow-up Service for Low-to-Medium Risk Hypertensive Patients: A Randomized Controlled Trial',IEEE journal on Information Technology in Biomedicine, Vol. 12, no.6.pp. 780 – 791.

[12]Neethu Mathew, 'A Boosting Approach for Maternal Hypertensive Disorder Detection',(2018),IEEE journal of computer science and engineering, volno.53,no.3,pp.7-21.

[13]Raneshkumar naha, Saurabh garg ,prem prakash jayaraman, yong xiang and rajiv ranjan, (2018),'Fog Computing: Survey of Trends, Architectures, Requirements, and Research

Directions',IEEE journal of school of technology, environments and design,Vol.23,no.3,pp289-316.

[14]Sandeep Sood K. and Isha Mahajan (2019), 'IoT-Fog based Healthcare Framework to Identify and Control Hypertension' IEEE Internet of thing journal,Vol. 6, no.2,pp.1920 - 1927.

[15]Tuan Nguyen Gia, Mingzhe Jiang Amir-Mohammad Rahmani, Tomi Westerlund, Pasi Liljeberg, and Hannu Tenhunen(2017) , 'Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction',IEEE journal of Computer and Information Science,vol.25,no.5,pp.222-230.

[16] Raja, K.S., Kiruthika, U. An Energy Efficient Method for Secure and Reliable Data Transmission in Wireless Body Area Networks Using RelAODV. Wireless Pers Commun 83, 2975–2997 (2015). https://doi.org/10.1007/s11277-015-2577-x