International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 12 | Dec 2019 www.irjet.net p-ISSN: 2395-0072

Enhancing Data Security in IoT Healthcare Services using Fog Computing

Saloni Alhat[1], Nikita Bangal[2], Aishwarya Gaikwad[3], Smita Khairnar[4]

[1]*Saloni Alhat, Dept. of Computer Engineering, PCCOE, Maharashtra, India*
[2]*Nikita Bangal, Dept. of Computer Engineering, PCCOE, Maharashtra, India*
[3]*Aishwarya Gaikwad, Dept. of Computer Engineering, PCCOE, Maharashtra, India*
[4] *Professor Smita Khairnar , Dept. of Computer Engineering, PCCOE, Maharashtra, India*

Abstract - *Security of the data is also major challenge in cloud. Fog computing is the answer to overcome the challenges. Fog node works at the edge side and enhances data security, accuracy, consistency and reduces the latency rate which is an important factor for application like medical data. In this paper we will detect the heart disease by using sensors and pulse rate. The data detected will be stored in the fog node .The result would be display by the system as well as report will be sent through mail to the patient. The data collected from it is being encrypted in fog node using Advance Encryption Standard (AES) algorithm and it is send to cloud. Therefore, the security of the health care data is enhanced using Fog computing.*

Key Words*: *Internet of Things, Fog computing, Advance Encryption Standard, Sensor, Pulse Rate, Heart Disease.

1. INTRODUCTION

With the advancement in IoT devices particularly in healthcare sector, huge amount of data is collected from different sensors and all this data are transferred and stored in cloud. System ensure safety on cloud from attacker or insider, this can prove helpful in government organization or any IT-industry. The data collected from it is being encrypted in fog node using Advance Encryption Standard (AES) algorithm and it is send to cloud. Fog computing overcomes the scalability and reliability issues which is there in the traditional IoT-cloud architecture. In Medical Diagnosis it is important to measure accurate pulse rate for prediction of diseases. So, continuous monitoring of pulse rate with portable low cost system will always be in need. System will take the information about the pulse using pulse rate sensor and predict the chances of heart attack.

Therefore, the security of the health care data is enhanced using Fog computing.

1.1 Project Objective

1. To Predict the Heart Diseases using Random Forest technique.
2. To provide security to data using AES Algorithm.
3. To reduce storage in cloud and fast retrieval.
4. To improve efficiency.
5. To reduce the amount of data that needs to be transported to the cloud for data processing, analysis and storage.

2. Problem Statement

To enhance the data security in IoT disease prediction system using fog computing. System will take the information about the pulse using pulse rate sensor and predict the chances of heart attack. The data entered by patient will be stored on cloud and get secured by using fog computing. System will make use of random forest classifier to predict percentage of chance of heart attack and will use AES algorithm to secure data.

2.1 Existing System

Currently in existing system the network such for computing tasks can be executed, and provide tradeoffs with respect to requirements relevant to healthcare. Review indicates that (1) there is a significant number of computing tasks in healthcare that require or can benefit from fog computing principles, (2) processing on higher network tiers is required due to constraints in wireless devices and the need to aggregate data, and (3) privacy concerns and dependability prevent computation tasks to be completely moved to the cloud. Hence, security is the major problem in existing system.Therefore; this system is not a very good way of securing data.

2.3 Proposed System

In this system we are implementing Random Forest Algorithm to carry out diagnosis of heart disease and AES algorithm to secure the data generated by system.

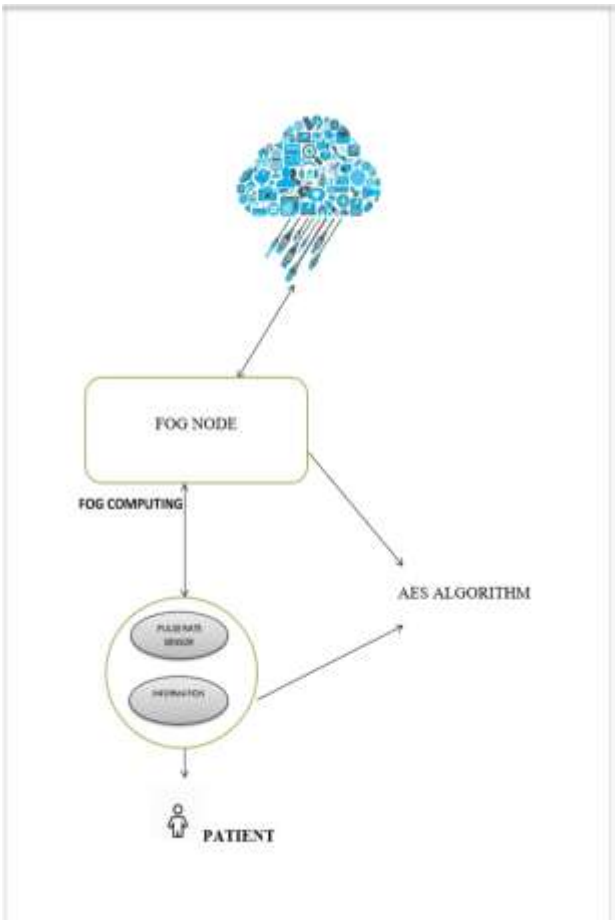

Fig .1- Proposed System

2.4 Mathematical Model

Let S be a system which predicts the percentage of getting heart attack. S is defined as

S={ I, A, O }

Where,

I= Input, which pulse rate sensor can sense

A= constraints for heart attack

F= Fog computing and security

O= Output, Percentage of getting heart attack

Flow of system:

1. Pulse sensor sense the input data of the patient. Also it will take the details of the patient.

I= {Pi1, Pi2, … ,Pin}

2. Save the data on cloud and maintain a fog node for security. Apply the constraints on input.

A= constraints for heart attack

A={A1, A2, … , An}

F= Fog node

F={F1, F2, …, Fn}

3.O= Output, Percentage of getting heart attack

O={O1, O2, …, On}

3. Techniques and Algorithm

3.1. AES Algorithm

Advanced Encryption Standard (AES) algorithm is one on the most common and widely symmetric block cipher algorithm used in worldwide. This algorithm has an own particular structure to encrypt and decrypt sensitive data and is applied in hardware and software all over the world. It is extremely difficult to hackers to get the real data when encrypting by AES algorithm.

3.2. Random Forest

Random forest can be used as classification as well as regression task. Random forest algorithm is the combination of "Bootstrap aggregating method" and random subspace method to build various decision tree. Random forest is an ensemble classifier based on large number of decision tree. Each decision tree gives the individual outcome by analyzing the condition. The class having the more votes consider as a models prediction. It is a supervised machine learning algorithm.

To check the generalized algorithm in random forest, and upper bound is derived. This error is consisting of two parameter mainly,

1. The Accuracy of individual classifier.

2. The dependency between the individual classifiers.

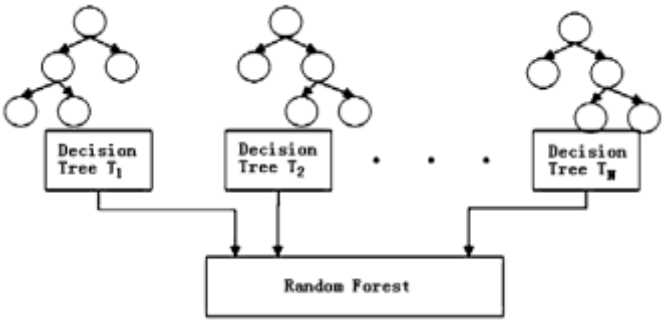

Fig .2- Random Forest

4. CONCLUSION

The System Analyse the pulse rate and Predicts the Heart Diseases. The data in the system is secured by using AES algorithm which is mostly used to encrypt the data. Stored data predict the patients health report by using random forest algorithm. System enhances data security, accuracy,

consistency, reduces the latency rate and enhances the overall quality of service. The data stored on the Fog can be stored in a secure way. The system maintains data integrity. System protects against misuse of real user data.

REFERENCES

[1] Yumnam Winnie, Umamaheswari E, D M Ajay, "Enhancing Data Security in IOT Healthcare Services using Fog Computing", International Conference on Recent Trends in Advanced Computing, 2018.

[2] Kraemer, Frank Alexander, Anders Eivind Braten, Nattachart Tamkittikhun, and David Palma, "Fog Computing in Healthcare–A Review and Discussion.", IEEE Access 5, 2017.

[3] Al Hamid, Hadeal Abdulaziz, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren, and Atif Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography.", IEEE Access 5, 2017.

[4] Alrawais, Arwa, Abdulrahman Alhothaily, Chunqiang Hu, and Xiuzhen Cheng, "Fog computing for the internet of things: Security and privacy issues.", IEEE Internet Computing 21, 2017.

[5] Reddy Prasad, Pidaparthi Anjali, S.Adil, .Deepa,"Heart Disease Prediction using Logistic Regression Algorithm using machine Learning", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-3S, February 2019.

[6] Rahmani, A. M., Gia T.N., Negash B., Anzanpour A., Azimi I., Jiang M., and Liljeberg P.: Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Future Generation Computer Systems, 78, 641-658 (2018).

[7] Goyal, Abhishek, Kanika Narang, Gautam Ahluwalia, P. M. Sohal, Bhupinder Singh, Shibba T. Chhabra, Naved Aslam, Bishav Mohan, and Gurpreet S. Wander, "Seasonal variation in 24 h blood pressure profile in healthy adults-A prospective observational study." Journal of human hypertension, 2019.

[8]https://blog.oureducation.in/cloud-computing-anemerging-technology

[9]http://internetofthingsagenda.techtarget.com/definition/fog-computing-fogging

[10]https://www.youtube.com/watch?v=pdmyYbdLnkI