International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

# Preserving the Privacy of Chronical Big Data Using Fog and Cloud Computing

**Prof. Chikane Yogesh[1] , Komal Thorat[2], Shweta Dawkhar[3], Mansi Kulkarni[4], Samiksha Wale[5]**

Professor, Department of Information Technology, Amrutvahini Engineering College, Sangamner, Maharashtra, India[1]

Student, Department of Information Technology, Amrutvahini Engineering College, Sangamner, Maharashtra, India[2,3,4,5]

**ABSTRACT***:* With the tremendous growth in medical big data there are increasing opportunities in the healthcare sector. We refer to this medical data as big data which is having 4v's as their properties. Storage and evaluation of big data is flexible and scalable on the cloud but at the same time there are issues in security such as data theft attacks. The problem of security can be resolved by using the technique called Fog computing. The data can be stored the security by using implementing decoy technique in fog. Additional security provided by encryption. In this paper, the main focus has been given to the evaluation and security of medical data. We have to come up with a new technology named Fog computing which also concentrates on processing of data.

**KEYWORD***:* Medical Big Data, Storage and evaluation, Cloud Security, Fog computing, Decoy Technique, Encryption.

## I. INTRODUCTION

Medical data has a continuous growth in healthcare sector. Such Medical Data contains the properties of big data such as Volume (exponential growth in data), Velocity(takes different forms) and Variety(changes in data are frequent) and Veracity(data can be incomplete or noisy). Most of the medical data is unstructured hence there is a need for preprocessing of the data for analysis. Analysis of data can be done by using data algorithms and tools. ETL (Extract, Transform and Load) is also a method for preprocessing of structured ,unstructured and semi-structured data. Different visualization method is also used for better understanding of data[1].

Certain challenges exists in the big data which are storage, searching , sharing and analysis of data. The healthcare cloud would make it much easier to store a huge amount of medical data but at the same time data on the cloud can access easily. Another issue occurs is that to access data from the cloud requires more time. To overcome security and latency issue Fog computing comes in a picture "Fog computing is a technique that provides storage, processing and communication services close to end-user". Fog can also used to provide security by placing decoy files in it. Decoy files contain fake information that is given to unauthorized access. Additional security can be given by using encryption. Encryption can be done using different algorithms such as Elliptic Curve Cryptography(ECC) and Blowfish algorithms[2].

Fog computing can also be used as a temporary method of storage. Due to the properties, such as ubiquitous, convenient and on-demand network access to a shared pool of configurable computing resources, cloud computing is mostly used to share a bulk amount of data but it has issues such as data security and confidentiality. Fog can be used to store the data collected by fog computing node as shown in fig1 [3]. The data security issue is solved by using decoy technology in fog. Decoy document or also called honeypot contains bogus information which similar to the original information and it is used to mislead an attacker hence securing original information. It will given to the unauthorized access once it is detected [4]. Decoy document can be generated by using a different methods such as random generator method, swapping of numbers, randomly adding or subtracting a number, etc.

Encryption is used for additional security in fog. ) Encryption is the process of converting the plain text to cipher-text. Different algorithm for encryptions is AES (Advanced Encryption Standard), DES(Data Encryption Standard).

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

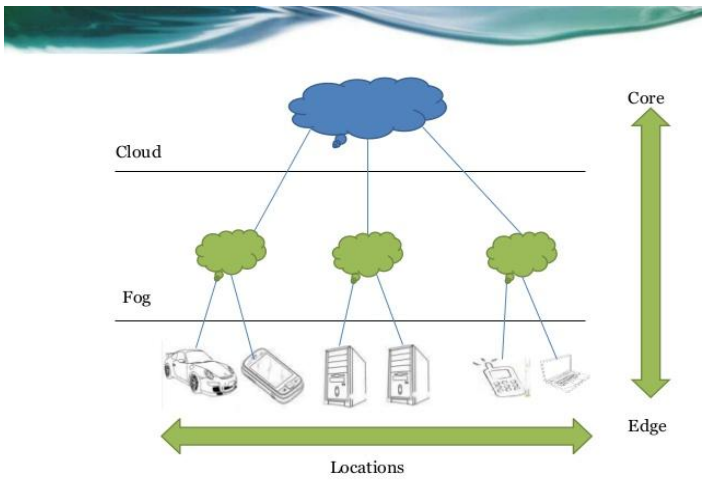


Fig 1:- Hierarchy of Network

## II. LITERATURE SURVEY

This section presents a comprehensive study on the evaluation, storage and security of a big data. A large amount of unstructured data can be pre-processed by using ETL. Extract is nothing but reading data from the database. In this process data is collected from multiple types of sources. Transformation of data includes cleaning,filtering,validating and applying rules to extracted data. Extracted and Transformed data is loaded to database in loading. Different visualization methods of data such as Treemap(Hierarchical grouping), Circle Packing (arrangement of circles), sunburst (space-filling visualization uses radial layout) . For chronic disease monitoring and early warning two diseases Diabetes mellitus and Asthma are used[1].

How fog can be used for security is discussed in [2].Placing the decoy document in the same environment where it is created is one method. After registration at the time of login if the user enters the wrong password three times then automatically decoy file will be given. Another method suggest after successful login whether a user is authorized or unauthorized give him/ her decoy document. Legitimate user will identify that the file he/she downloaded is not original so he/she will move to the next step and answer some security questions and download the original file. Another method similar to this is users have to answer the security question first after a successful login. If all answers are correct, original file will be given otherwise decoy document will be given. Fog can be also used for the storage of data. The main characteristics of fog computing are [1]:Low Latency:-Less delay in the accessing the data [2]Heterogeneity:- Fog nodes can be deployed in the different types of environments. [3] Support for the mobility:- It communicates directly to the smart devices eg.Sensors , Mobile devices[4] Interpretability:- fog component must be able to interoperate to support of the different services. [5]Real-time communication:- It gives speedy service[3].In[4],the limitations of cloud computing system and hence need of Fog computinmg is explained. Limitations in cloud computing system are [1]:- The application that require very low and predictable latency [2]: Geographically distributed application [3]:- Large scale distributed computing system.

Other than decoy file security will be also given by Encryption. DES is used for encryption. It is a symmetric key algorithm that uses a 56-bit key and block size is 64 bit. This algorithm is not secure because the key size of the 56-bit could be brute-forced which is easier to crack using Differential Cryptanalysis, Linear Cryptanalysis and improved Davies Attack.

The predecessor of the DES algorithm is 3DES(Triple Data Encryption Standard ) in which key size is increased to 56 or 112 or 168 bit and block remain the same as 64 bits. 3DES does not function properly in the software applications. To overcome thes problems, AES is used. AES also uses a symmetric key encryption method. AES has 3 key sizes : 128 bits,192 bits and 256 bits. It has a fixed block size of 128 bits. AES is considered as a most secure algorithm for encryption [5].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

## III. PROPOSED SYSTEM

The proposed system have two methodologies: Admin and User.

1] User :

- Register/ sign up
- Username
- Password

Personal Details:-i] Name ii] Address iii] contact no iv]Email-Id v] Date of Birth.

Sign in

- 
- Username
- Password

Select Basic Symptoms

- Submit

Fill the next level parameter

- Submit.

Download the report from my profile.

2] Admin

Log in
Active patient status/ delete patient status
Suggestion of tests
Suggest hospitals and precautions.
Logout.

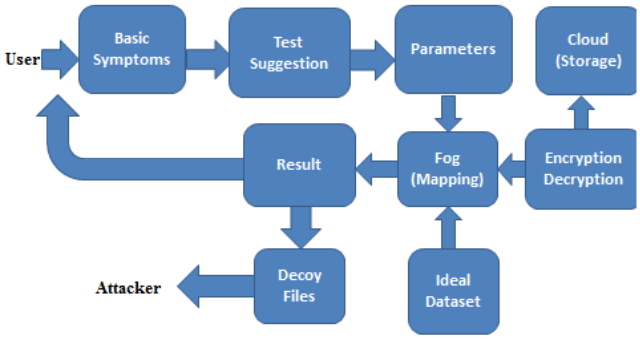


Fig 2:Flow of the System.

1]User:
User will register to the system and then login.While registration he/she has to fill personal details also.

2]Basic symptoms:
After successful registration the user select basic symptoms from which he/she is suffering from.

3]Parameters:
After tests, parameters will be obtaine such as cholestrol,Resting blood sugar, Fasting blood sugar, Blood pressure,etc. These parameters are mapped with ideal dataset whichwe have already stored.

4]Fog:
In fog ,mapping is done and also decoy file are generated. Reports are also provided to the patient from fog.

5]Decoy Files:
Decoy files contain incorrect information which is used to mislead attacker.These
are created using randomely adding and subtracting a number from original parameter.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

6]Encryption/Decryption:
Encryption of the report is done for security and also decryption is done in case patient requests report.

7]Cloud:
Encrypted reports are stored on cloud for anytime access.

In the proposed system as shown in fig.[3]

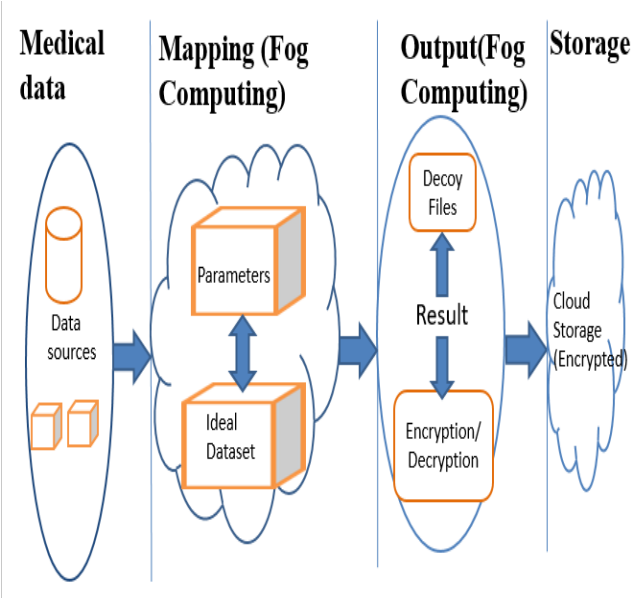


Fig 3: Architecture of Proposed System.

Stages of chronic disease will be given by mapping with an ideal dataset and a report will be provided to the patient through mail. All this processing is done in fog. Report of the patient is secured by using decoy file in the system and stored in an encrypted format on cloud . From fog the report containing stage of chronic disease will be provided to the patient with suggestions of hospitals through mail . In case if patients wants to download report again then he/she can download it from his/her profile. If patient requests the report to download from profile then automatic Decryption is done and patient can download it.

How the whole system will work is shown in fig.[3] in which different smart devices sends data to fog for processing and after processing will send to cloud from fog.

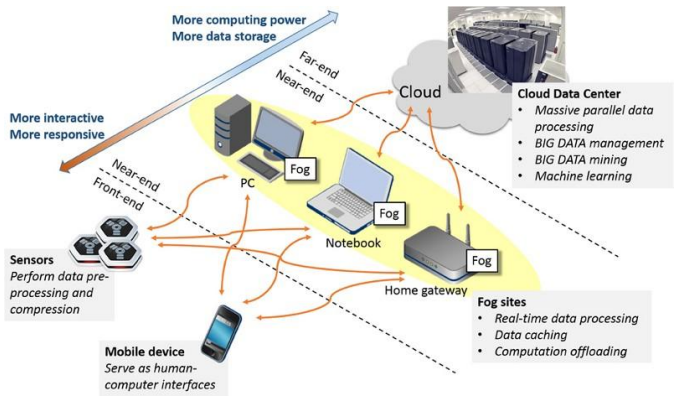


FIG: CONCEPT OF FOG COMPUTING.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

**ALGORITHMS**

**Advanced Encryption Standard(AES):-**

Input:
128 bit /192 bit/ 256 bit input(0,1)
Secret key (128 bit ) + plain text(128 bit)

Process:
10 cycles of repetition for 128 bit key
12 cycles of repetition for 192 bit key
14 cycles of repetition for 256 bit key

Output:
Ciphertext and Plaitext.

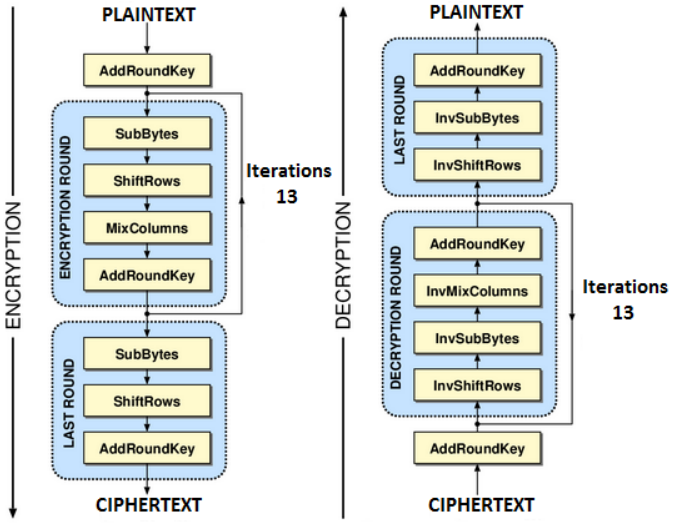


Fig 4: Architecture of AES

Each round consist:

**1] The SubBytes step:**

In this transformation step,the intermediate ciphertext undergoes various substitution operations. It is used for encryption process.

**2] The ShiftRows step**

In this transformation step,the intermediate cipher text undergoes various row-wise transposition operations.

**3]The MixColumns step:**

In this transformation step,the intermediate cipher text undergoes various column-wise transposition operations

**4]The AddRoundKeystep :**

In this transformation step round key is generated and XORed with the intermediate ciphertext.It is used both in encryption and decryption.

**5]InvShiftRows:**

This is inverse of shift row operation.

**6]InvSubBytes:**

This is inverse of SubBytes operation.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

**7]InvMixColumns:**
This is inverse of MixColumns operation.

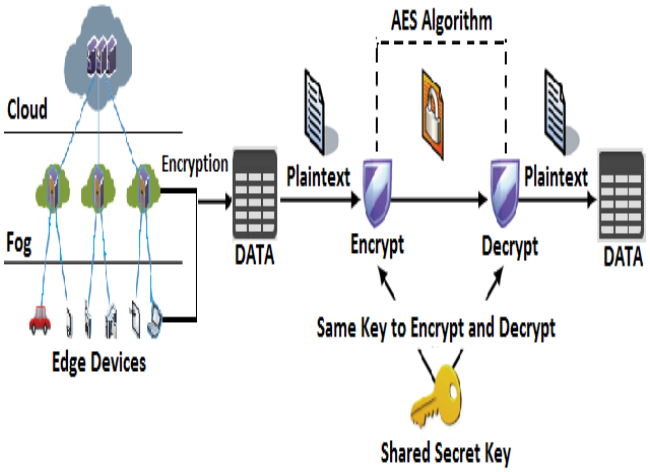


Fig 5:Encryption and Decryption Process

**Decoy File Implementation :-**

For the implementation of heart disease and diabetes we have used the random number generator method .It randomely generates the false values to the actual parameter which are stored in decoy files.The code for generation of decoy file is as follows:

```
String _lename=username + ":txt";
FilemyObj3 = newFile("D : DecoyFiles□+filename);
if (myObj3:createNewFile())
System:out:println("Filecreated : " + myObj3:getName());
else
System:out:println("Filealreadyexists:");
FileWritermyWriter = newFileWriter("D : DecoyFiles□+filename);
UserDaodao = newUserDao();
Stringdd = dao:key();
System:out:println("RandomNumber : " + dd);
intkey = Integer:parseInt(dd);
intbp1 = Integer:parseInt(bs);
floatchlevel1 = Float:parseFloat(fbs);
intbs1 = Integer:parseInt(bs);
intnewbp = bp1 -key :
floatnewchlevel = chlevel1 - 2;
intnewbs = bs1 + key;
myWriter:write("DiabetesDiseaseParameter □ " + "Haemoglobin : " + newbp +
";BloodSugar : "+newchlevel+"; FastingBloodSugar : "+newbs+"; UrineTest :
" + urine + "; FamilyHistory : " + fh + "; Age : " + age);
   myWriter:close();
```

## IV. CONCLUSION

In this paper we have work on evaluating the stage of chronic disease of the patient and most important is to give security to the patient's sensitive data by using the decoy technique. With the purpose of reducing the latency and giving security using decoy files we have come up with a new technology called fog computing. Advanced Encryption Standard in fog computing is also used for additional security.

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 6, June 2020 ||

## REFERENCES

[1]RongHeng Lin, ZeZhou Ye, Hao Wangy, BudanWu :Chronic Diseases and Health Monitoring Big Data:A Survey
[2]HadealAbdulaziz Al Hamid, 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 aFog Computing Facility with Pairing-BasedCryptography
[3]Sirisha Sanatha1, Swathi Amancha:AN ENHANCED CLOUD STORAGE METHOD: FOGCOMPUTING
[4]Arwinder Singh1, Abhishek Gautam2, Hemant Kumar3, Er. C.K. Raina4: Decoy Technology in Fog Computing.
[5]Akhilesh Vishwanath,Ramya Peruri,Jing (Selena) He:
Security in Fog Computing through Encryption
[6]T.Nagamani, S.Logeswari, B.Gomathy:Heart Disease Prediction using Data Mining with Mapreduce Algorithm
[7]Min Chen, Jun Yang, Yixue Hao, Jing Zhang, and Chan-Hyun youn: 5G Smart Diabetes:Toward Personalized Diabetes Diagnosis with Healthcare Big Data Clouds.