International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume 9 Issue 10 October 2022 Regular Edition E-ISSN: 2349-7084

Privacy model to secure Chronical big data: Fog Computing

Yogesh R. Chikane[1*], Rashmi Soni [2]

[1*] Research Scholar, Department of Computer Science and Engineering Oriental University, Indore

[2] Research Supervisor and Associate Professor, Department of CSE Oriental University, Indore

e-mail: yogeshchikane2006@yahoo.com, drrashmicse@gmail.com

*Corresponding Author: Yogesh R. Chikane

Available online at: http://www.ijcert.org

Received: 15/09/2022, Revised: 23/10//2022, Accepted: 30/10/2022, Published: 04/11/2022

Abstract:- With the tremendous growth in medical data, there are increasing opportunities in the healthcare sector. In this research, the main focus is on providing the current stage of disease and securing sensitive data on the cloud. After taking the patient's input in the form of symptoms of a chronic disease, we are going to make test suggestions. Parameters that are obtained from the results of the tests are mapped to ideal values stored in the database. After mapping a stage of chronic disease, a report will be provided to the patient, and the report will be stored on the cloud in encrypted format. All this data management is done in the cloud, and only solutions are saved there. Fog computing gives fast storage and processing to correspondence benefits near the end client. It is used mainly for reducing latency. Latency is nothing but improvement time. Fog computing is also used to deliver protection by making use of decoy files. The decoy file contains fake or incorrect information that is used to mislead the attacker. It is given to unauthorized access. In this paper, the main focus is on providing the current stage of disease and securing the sensitive data of a patient, which is stored in the cloud. After taking the input in the form of text from the patient, we are going to map this information with ideal values stored in the database. All this data processing is done in the cloud, and only the results are stored there. Fog computing provides storage, processing, and communication services close to the end user. It is used mainly for reducing latency. Healthcare cloud computing faces security issues such as data theft attacks. To decrease the value of these data theft attacks, encryption and decryption are used, and additional security is provided by placing decoy files in the fog. The decoy file contains incorrect information, which we are giving to the attacker after successful decryption.

Keywords: - Cloud computing, Decoy file, Medical Big data, Fog computing.

1. Introduction

Enormous information sets out new doors for well-being and clinical areas. In our research work, I am going to take input in the form of text from patients. In fog, data received by the patient is mapped to ideal values stored in the database, which provides security to the sensitive data using decoy files. Encryption and decryption are used to reduce the value of these data theft incidents. Ongoing research involves patients with MBD in the medical services cloud utilising the decoy procedure with haze figures for facility. It contains a second display, which contains DMDB, which appears to the

assailant as though it is the OMDB. Fog computing is used mainly to reduce latency[1].

Decoy files are used to confuse the third party and assure them that the data and information about the patient they have is correct. With the consistent advancement of clinical data, the extension of clinical information speeds up, and the inclusion territory increases. The coming of the enormous information period sets out new doors for well-being and clinical spaces. As we all know, massive information contains 4V, that is, quantity, speed, variety, or accuracy. The huge amount of clinical information has four highlights. For volume, an ordinarily refereed measurement from EMC said that 4.4 zeta bytes of information existed universally in 2013. That count is anticipated to reach 44 zeta bytes by 2020, as it dramatically increases every year. For speed, the person observing information is creating each second. For assortment, the clinical space contains numerous potential huge information sources, for example, the advanced clinical record, MRI, CT, well-being checking information, and genome information.

For veracity, clinical information may be deficient, one-sided, or even loaded up with commotion. Also, clients can't use bits of knowledge. Massive information in medical services refers to sets of automated medical well-being information that are huge and, what's more, complex. Because of their tremendous volume and intricacy, it is troublesome (or infeasible) to deal with those informational collections utilising conventional programming and additional equipment. What's more, the volume of mixed-media clinical large information (MBD) and productive availability of these datasets make it compelling. Like distributed computing, medical distributed computing also has different confidentiality issues, the most important of which are: technical and legal issues, data protection, security confirmation, indirect network health issues, non-compliance with security standards, and programming permissions [2].

Every one of these issues has various difficulties that can be briefly talked about as follows: The moves identified with legitimate and strategy issues in distributed computing are: obligation, appropriate law, consistency, copyright, data portability, and information insurance.

To get patient MBD in the medical services cloud, utilise the bait strategy with a mist figuring office. It fills in as a subsequent exhibition to contain distraction medical big data that appears to the assailant as though it is the first medical big data. In contrast to different strategies, where the fake documents are considered when an assailant is recognised as getting to the framework, in our approach the imitation records are recovered from the start to guarantee good security. They would have to sort out some way to interpret the first display. Thus, our information makes sure that user data is abbreviated in the procedure. There is no convincing explanation for pressure if the client is an assailant, since naturally it offers the bait of huge information exhibition straightforwardly to any client and keeps the first one covered up, which is simply made accessible to a real client after effective confirmation.

Cloud Computing:-

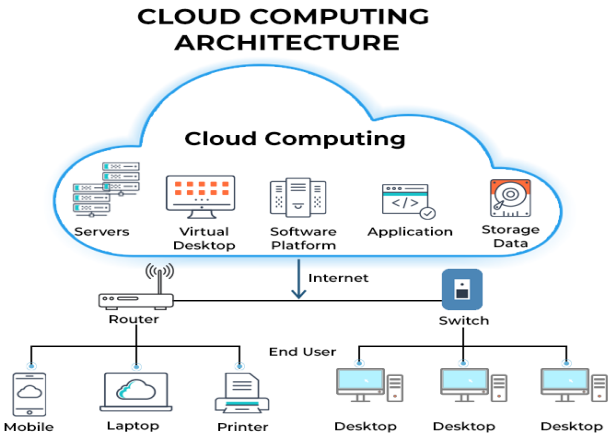

Figure 1:- Architecture of Cloud Computing [3]

As an alternative to storing files on a storage tool or hard drive, a user can keep them on the cloud, making it possible to access the files from anywhere if they have gained access to the web. Front-end and back-end are the two parts of the cloud that can be distributed into two separate layers as mentioned. The layer with which users interact is called the front-end layer. This layer enables a user to access the data that has been kept on the cloud through cloud computing software.

To guarantee continuous connectivity among devices connected via cloud computing, the central servers use software called middleware that acts as a bridge between the database and applications.

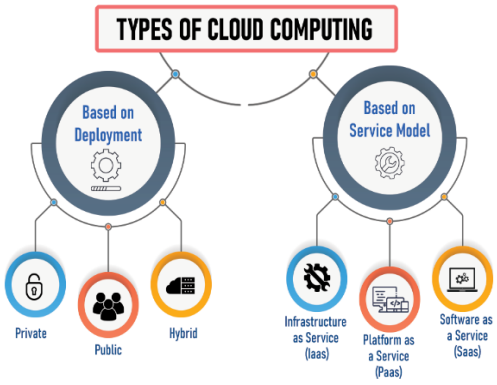

Figure 2: - Types of Cloud Computing [4]

Private cloud:-

In a private cloud, the computation services are recommended over a private IT network for the committed use of a single business. Also termed "inner," "enterprise, or "commercial cloud," a private cloud is usually managed via internal resources and is not accessible to anyone outside the organization. Private cloud computing supports all the benefits of a public cloud, such as self-maintenance, scalability, and flexibility, along with supplementary management, protection, and customization.

The disadvantage of private cloud, however, is that the company becomes accountable for all the management and preservation of the data centres, which can prove to be quite resource-intensive.

Public cloud:-

The public cloud refers to computation services offered over the Internet by third-party suppliers. Like private clouds, the services on public clouds are available to anyone who wants to use or purchase them.

Public clouds can help organizations save on buying, controlling, and maintaining on-premises infrastructure since the cloud service provider is responsible for managing the system. They also offer scalable RAM and adaptable bandwidth, making it easier for organizations to scale their storage needs.

Hybrid cloud:-

Combination of public and private cloud properties is nothing but hybrid cloud. The "best of both worlds" cloud prototype allows a shift of loads among private and public clouds as the computation and cost conditions change. When the requirement for computing and processing fluctuates, hybrid cloud allows businesses to scale their on-premises infrastructure up to the public cloud to handle the overflow while ensuring that no third-party data centres have access to their data.

In short, a hybrid cloud extends the benefits of a public cloud without its security risks.

Based on the service model, cloud can be classified into IaaS (infrastructure-as-a-service), PaaS (platform-as-a-service), and SaaS (software-as-a-service). Let's take a look at each one.

Infrastructure as a service (IaaS):-

Infrastructure as a service or IaaS is a type of cloud computing in which a service provider is accountable for delivering servers, storage capacity, and networking over a simulated interface. In this service, the user doesn't need to manage the cloud infrastructure but has control over the storage, operating systems, and deployed applications.

As an alternative of the client, a third-party supplier hosts the computer hardware, software package, servers, storage space, and other infrastructure components. The supplier also hosts the user's applications and supports a backup.

Platform as a service (PaaS):-

Platform as a service or PaaS is a type of cloud computing that provides a development and deployment environment in cloud that allows users to develop and run applications without the complexity of building or maintaining the infrastructure. It provides users with resources to develop cloud-based applications. In this type of service, a user purchases the resources from a vendor on a pay-as-you-go basis and can access them over a secure connection.

PaaS doesn't require users to manage the underlying infrastructure, i.e., the network, servers, operating systems, or storage, but gives them control over the deployed applications. This allows organizations to focus on the deployment and management of their applications by freeing them of the responsibility of software maintenance, planning, and resource procurement.

Software as a service (SaaS):-

SaaS or software as a service allows users to access a vendor's software on cloud on a subscription basis. In this type of cloud computing, users don't need to install or download applications on their local devices. Instead, the applications are located on a remote cloud network that can be directly accessed through the web or an API.

In the SaaS model, the service provider manages all the hardware, middleware, application software, and security. Also referred to as 'hosted software' or 'on-demand software', SaaS makes it easy for enterprises to streamline their maintenance and support.

Cloud computing and artificial intelligence allow for the dynamic processing and storage of these large amounts of data. This data enables organizations to make informed decisions and protect themselves from vulnerabilities at both, business and technological levels.

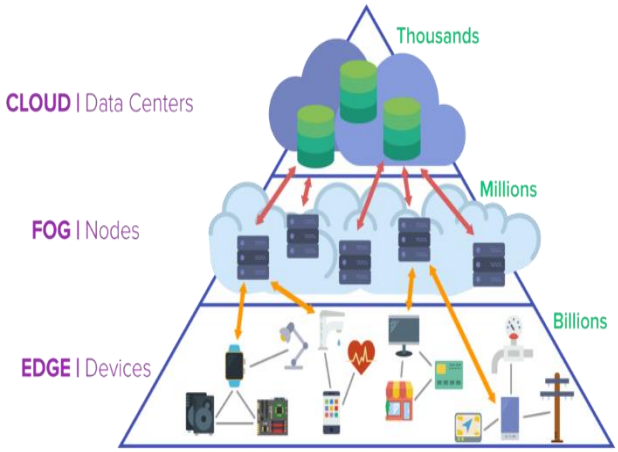

Figure 3:- Cloud, Fog, Edge Computing [5]

Let's consider the data sent by a temperature sensor in a factory line. The temperature recording can be pushed to the cloud every second with a service checking for fluctuations. But a more intelligent way of storing this information would be to check if there have been any temperature changes in the last few seconds. When a temperature change is noticed, the data is pushed to the cloud for storage to verify the proper operation of the production line. The temperature may take up little space, but this kind of scenario is also common with devices such as CCTV cameras that produce large video and audio data.

Edge devices include routers, cameras, switches, embedded servers, sensors, and controllers. In edge computing, the data generated by these devices are stored and computed at the device itself, and the system doesn't look at sharing this data with the cloud.

Fog computing have a layer between edge devices and the cloud. The servers are connected to each other and centralized cloud servers, enabling the intelligent flow of information. These small units work together to handle pre-processing of data, short-term storage, and rule-based real-time monitoring. The fog computing architecture reduces the amount of data transported through the system and improves overall efficiency.

Fog processing, is an emerging perspective that gives storing, dealing with, and correspondence benefits closer to the end customer. It diminishes dormancy, gives area mindfulness, and supports high-thickness remote organizations. Providing information and storing it in the organization's local storage to get closer to the customer is considered one of the main atomization tasks[6]. End clients are associated with multiple hubs, which are called "edges", hence they are also called "edge processing". Fog figuring doesn't supplant distributed computing

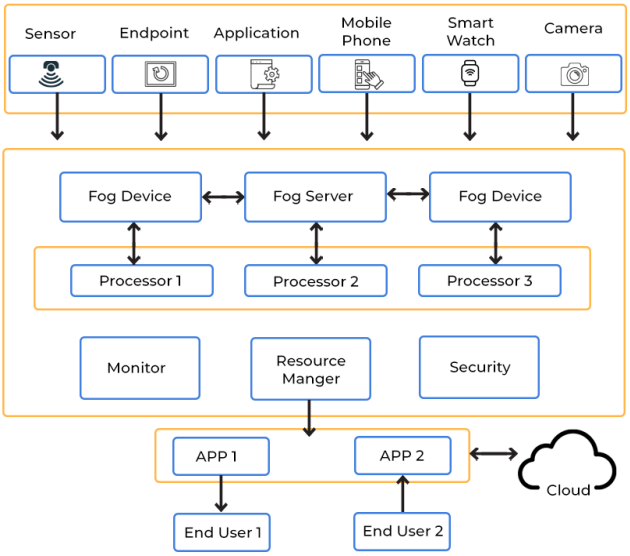

Figure 4:- Fog Computing Architecture [7]

2. Related Work

In [8] the author focuses on the technology development of the data science and the network technology. With the innovation advancement of the information science and the organization innovation, the world has ventured into a major information time. Clinical zone incorporates huge measure of information which is appropriate for information investigation. Bunches of examination work in clinical enormous information has been done as of late, focusing on information assortment, information examination and representation. very few research work gives a full review of the clinical huge information on constant sicknesses and well-being observing. To get a complete comprehension of huge information in enormous clinical information, particularly in constant infections and well-being checking territory.

This paper [9] explores on going examination endeavours, and leads an extensive outline of the work on clinical enormous information. It centres on the full patterns of the huge information handling, which incorporates clinical large information pre-processing, huge information devices and calculation, large information representation, security issues in huge information. It additionally attempted to fill the hole between regular huge information innovation and clinical unique necessities by breaking down detail execution

of clinical enormous information. As far as we could possibly know, this is the principal study that objectives the constant sicknesses and wellbeing checking huge information technologies. Index Terms |medical enormous information, persistent sicknesses, wellbeing observing, information analysis, data representation.

Author focuses on the utilization of large information, distributed computing for getting the information has become the customary technique for information stockpiling. As distributed computing is step by step developing with its prominence and its consideration on the whole different backgrounds, its contribution tremendous number of administrations to the clients. This is the basic explanation for the development of product organizations in this innovative direction. Due to the large number of customers in this field, the honesty, security and confidentiality of information are at risk. Distributed computing is not only the basic model we are familiar with before, but it also incorporates a host of registry technologies, methods, and ideas such as software-oriented architecture, virtualization, and other things that depend on the network.

Virtualization is about using virtual assets to shape virtual adaptation in the fog and cloud. Even in this cloud, we have security components such as personality, verification, approval, worker work, key repair, but they are not enough for our security clauses. Somehow, information security is related to high decryption progress or hacking issues. This is how the "fog management" perspective came to Limelight. Haze Digital is prominently known as Hazing and Edge Computing, it is a model in which data, care and applications are usually assembled on the end client or device, for example on the associated (edge) side, rather than basically focusing on the cloud .

Due to pay-as-you-go plans and various attributes (for example, on-demand, self-interest, bundled assets, and fast flexibility). In the fog cloud, adaptive assets extend to the edge of the frame, such as smaller devices, cool things, remote sensors, and other Internet of Things (IoT) devices to reduce latency and frame blocking. IoT devices use advancements in interconnection such as radio frequency identification (RFID) and wireless sensors and participant networks (WSAN) to exchange data via the Web, and they are gradually 6 becoming more coordinated in our lives. Enthusiastic urban area, smart agriculture, smart grid, sharp city, splendid power grid, electric current engine, flying robot, fight against illegal fishing, power frame, etc.

In [10], the author focuses on, telemedicine is an arising medical care administration where the medical care experts can analyze, assess, and treat a patient utilizing telecom innovation. In order to investigate and evaluate patients, clinical welfare specialists must access the patient's electronic medical record (EMR), which can contain a wealth of visual and audio information, including X-rays, ultrasound, CT examinations, MRI reports, magnetism, etc. For efficient access and supporting portability for medical experts and patients, EMR must be stored in a large medical cloud storage. Ignoring the universality of clinical considerations, the cloud faces clear and unmistakable security issues; for example, data theft attacks may be considered the most authentic security portal for clinical welfare data in the cloud.

In this paper [11] the basic centre has been given the use of the haze computing office to obtain private information about medical services in the cloud. For this reason, considering bilinear hybrid cryptography that can create aggregate keys between individuals and securely negotiate with each other, a third-party single-round key verification scheme has been proposed. Finally, by implementing distraction techniques, securely obtain and store information from private medical services. Index term Key management; security and privacy; medical big data; computing in the fog; peer-based cryptography; decoy technology.

In [12] Distributed computing is considered as quite possibly the most energizing innovation 7 as a result of its adaptability and versatility. The primary issue that happens in cloud safety. To conquer the issues or issues of safety, another procedure called mist registering is developed. Since there are security issues in the fog even when getting mixed data from the cloud, we use AES estimation to perform encrypted collaboration to verify its mitigation capabilities. So far, for our research, AES computing is the most common secure encryption interaction considers three different types of data sets and applies independent encryption techniques to these data sets. At the time of approval, all data in the dataset was clearly scrambled and decoded. I accept Android Universal as an edge device and pass the encryption of the data set. In addition, if all information is efficiently encoded and decoded along with time, client load, response time, and memory utilization that exceeds the record size, then the encryption performance of the selected dataset is evaluated for ensure its accuracy. Therefore, the best and most pessimistic scenarios in the data set were investigated, and the rationality of AES in the fog was evaluated accordingly.

In [13] the healthcare for data computing fog computing add the importance in the managing significant number of tasks, processing the higher network and in the aggregation

of the medical data and privacy concern and integration of the data in patient concern. Fog computing and synonymously is edge computing is very important to perform different tasks like reduce latency, privacy, energy efficiency, bandwidth, scalability, dependability etc. in different types of the networks for healthcare applications.

In [14] the storage location and the end user might have the major issue in the latency in some of the critical cases. Fog computing is the one of the best solution for such types of the problems. It is very easy and fast way by using the fog computing. Fog computing able to provide the services by putting the data ate edge of the network which is closer to the end device and the end user. By using fog computing we cannot replace the cloud storage but it will provide the safe and faster way for the communication between the end device and user.

In this paper [15] the author explains the Cloud computing is one of the most famous technologies in data storage and operation, but security is the main issue. Fog Computing will resolve this problem. Even there is some security issues in fog computing as well so maximum security can be provided by involving the cryptography in the fog computing. Different encryption techniques can be used In the scenario. In this research they have suggested the existing techniques available can be used to provide the security in the fog and cloud computing. Advanced encryption standard (AES) technique suggested here.

Need of the healthcare organizations to use the data significantly to improve the quality and efficiency of the service and scale the system explain in the paper [16]. With the help of the Big data the 8 problems of the patients can be resolved as different tools and techniques are available for the analysis of the data also the prediction of the disease and facility can be easily made available with help of the big data. Big data challenges, applications and Opportunities are explained here and techniques and technologies are using for the medical big data as well.

The explain in the paper [17] basically every organization and industry data management, manipulation is important task and in current era the way is changed and become somewhat easier due to the big data. Big data has ability to change the way of the service of the patients in the sense of the output, prediction and prevention of the disease. Also it is essential that to provide the privacy and security the patient's sensitive data. In this research they focused the different issues related to the privacy and security of the patient medical data.

In this paper [18] Detection of the masqueraders is very difficult because they pretending themselves as a authenticate user and misusing the system or data. Decoy document deployment is the interesting way to secure the file from such inside attacker. This is trap based way for detecting the masquerade attacker. System will confuse the attacker regarding the contents and the location of the file also.

This is a better choice for cloud computing on a smaller network[19] . It will reduce end-user traffic to the cloud. The fog system is close to the computing data source, and communication will not be delayed.

In [20] the author explain the significance of the the Cloud computing regarding the cost reduction and eliminate system administration functions, but it also has certain limitations. These limitations stem from the massive and unpredictable network latency and undefined security issues that host cloud data centers on the Internet, because sensitive data is now entrusted to end users. Because the term fog computing is managed by CISCO on a distributed network. It is a virtualization platform that can provide better services and minimal delays to provide quality services.

In [21], the author focused on the comparison in between the cloud computing and the fog computing. They have suggested here fog have more advantages over the cloud computing. The difference between fog and cloud computing lies in the scheme, layout, management and equipment of the association and the end users. By consuming low network bandwidth, it is more flexible and better for data processing services.

3. Noteworthy Contributions in the Field of Proposed Work

3.1 Problem Statement:

In this research work, I am going to take the input in the form of text from patient. Input is nothing but the symptoms of the chronic diseases from which patient is suffering from. Chronic diseases are nothing but the diseases which persists for long time. Examples of chronic diseases are heart disease, arthritis, kidney disease, AIDS ,etc. After taking inputs, I am going to map the data from patient with the ideal datasets which I have stored in the database. The standard datasets for chronic diseases are downloaded from UCI machine learning. Mapping of data with ideal values is done in fog. Fog processing is an emerging perspective that gives storing, planning and correspondence benefits closer to the end customer. In our research work I mainly use fog for the

purpose of reducing latency. Latency is nothing but turnaround time. Turnaround time means amount of time taken to complete a process or complete a request. After mapping, from fog fast services are provided to the patient. I am going to provide a file containing current stage of chronic disease of the patient and cost of cure for that disease in different hospitals. Then this file is going to store on cloud for anytime access. This file is kept on cloud in encrypted format. For advanced security Decoy files are also stored in fog. Decoy files contain the bogus information which is used to mislead the attacker. If any unauthorized access is found then decoy file will be given to that access. By using this sensitive information if the patients which they do not want to expose remains secured.

Doctors in the hospitals have access to the patient's data on cloud. In any case, if patient wants to change the hospital then there will be no headache of carrying reports. Doctors will direct access the reports through cloud. In short, I will save the protection of patient's large information by utilizing fog processing and cloud for storing purpose and give early reporting to the patient for further treatment.

3.2 Scope

It is useful for getting the proper treatment with various choices and cost effective manner. Delicate data is protected and therefore there is no chance of information outflow. Services are provided as early as possible hence saving the time and patient also gets the treatment as early as possible. Awareness for chronic disease between users and helping them for secure their sensitive data and by providing best service information.

3.3. Objective:

1. Enhance integrity of patient data in cloud environment.
2. Utilize encryption algorithm to secure patient's sensitive data.
3. Enhance the processing speed and security using fog computing.
4. Design a security algorithm using the concept of decoy files to mislead attacker.
5. Provide comparative cost of different hospitals so one can choose hospital according to affordability.
6.

4. Proposed Method for the Duration of Research Work

4.1 Theoretical Background

Nowadays, there is tremendous growth in medical data. In this research work main focus is on providing the current stage of disease and secures the delicate information of a patient which is put away in the cloud. After taking the input in form of text from patient I am going to map this information with ideal values stored in the database. It is utilized chiefly for lessening the inactivity. Medical care cloud faces security issues for example, information burglary assault. To decrease the value of these data theft attack, encryption and decryption is used and also additional security is provided by placing decoy file in the fog. Decoy file contains incorrect information which we are giving to the attacker after detection of unauthorized access. At the last, proper detection of the disease with comparative cost of treatment in different hospitals is provided to the patients.

4.2 Architecture

Medical Data: In this phase the data related to the symptoms of the patients diseases such as heart disease and diabetes is gathered and test suggestion is given to them. Test suggestions include blood test, ECG, Holter Monitor test, AIC test, etc.

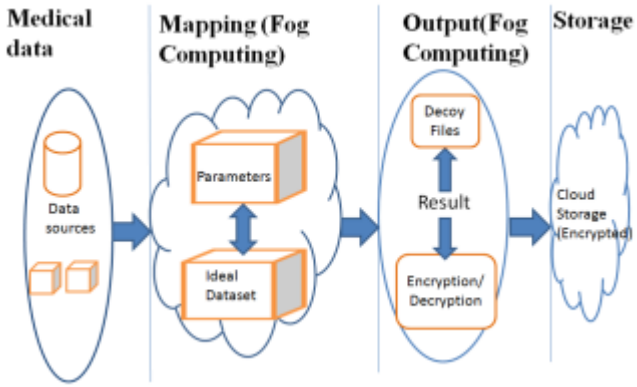

Figure5:- Architecture

Mapping: In this phase the parameters obtained from test results are mapped with ideal dataset in fog. Mapping is done with ideal parameters which will tell the patient's heart disease or diabetes result and then by applying some conditions patient will get the stage of the chronic disease.

Output: In this phase the report (stage of chronic disease) is given to patient and also some precautions and hospitals in the different cities are given to the patient through registered mail. Decoy file is created automatically created based on report and it contains random generation method and also encryption is done for purpose of security.

Storage: On cloud the encrypted files of the report are stored for anytime access. Cloud is one storage and storage is our fog that means laptop which also stored the encrypted files and decoy files.

4.3 Data Flow

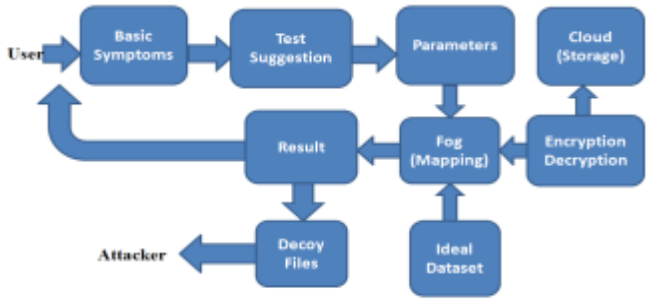

Figure 6:- Data flow diagram

1] User:

User will sign up to the system and then login. While registering he/she has to fill personal details also. If user fail to remember password then it can be retrieved by using forget password button. When user clicks on forget password his/her password will be provided to the mail.

2] Basic symptoms:

After successful registration the user select basic symptoms from which he/she is suffering from. Basic symptoms of heart disease includes chest pain and chest pressure, weakness, Pain in neck, jaw and throat, Irregular heartbeats, Extreme fatigue, etc. If patient choose diabetes then the basic symptoms for selection are Nausea, Fatigue, Extreme hunger, Blurred vision, Increased thrust, Patches of dark skin, etc.

3] Test suggestion:

Test suggestions such as blood test, Holter monitor test, ECG, AIC test, etc. are given to the patient. Patient will do it from hospital and then fill our next level parameters.

4] Parameters:

After tests, parameters will be obtained such as cholesterol level, Resting blood sugar, Fasting blood sugar, Blood pressure, any infection to heart, previous heart attacked for heart disease and for diabetes Haemoglobin level, blood sugar, Urine test 13 are obtained .These parameters are mapped with ideal dataset which I have already stored.

5] Fog:

In fog, mapping is done and also decoy files are generated. Our laptop is basically working as fog which will take input from smart devices and does all processing and then results are stored on cloud.

6] Result:

Result contains the stage of chronic disease and along with that it also contains some precautions and hospitals in the different cities for best treatment.

7] Decoy files:

Decoy files contain incorrect information which is used to mislead attacker. These are created using random generation algorithm for generating false values which will be different from original parameter.

8] Encryption/Decryption:

Encryption of the report is done for security and also decryption is done in case patient requests report. Encryption is the way toward changing over plaintext into figure text and unscrambling is the way toward changing over figure text again into plaintext. For encoding and decoding AES algorithm is used which is imported.

9] Cloud:

Encoded reports are stored on cloud for anytime access.

5. Expected Outcome of the Proposed Work

1. Reliability is attained in the situation of the system, that ensuring the patient role information is genuine, truthful and protected from illegal alteration.
2. Protection is delivered to the patient data using encryption and decryption algorithm.
3. Provide the easy and quick access to the patient data with the help of the fog computing.
4. More security is provided to the patient's sensitive with the help of decoy file algorithm.
5. Proper detection of stage of Chronical Disease which includes different hospitals in the cities with precautions by considering the cost of the hospitals.

6. Future Scope

The role of big data in the healthcare sector is going to become more vital with more demand from first going technologies like AI and machine learning. Also big data analytics will also become vital for healthcare organizations to operate with more efficiency and productiveness.

Moreover the availability of the healthcare training data for AI will also help wearable devices, patient monitoring also gives useful information to healthcare service provider to improve their services and help to get advanced healthcare facilities.

7. Conclusion

In this paper first propose a system that includes receiving symptoms entered by patient and mapping of these symptoms with the ideal values stored in ideal database. In addition we provide security to data using decoy file so it can secure.

The sensitive data which patient generally do not want to expose and also we provide additional security using encryption. Then we proposed a cost effective system which gives proper detection of stage of disease and gives comparative cost of treatments in the different hospitals. Patients can choose the hospitals according to convenience. As we are giving fastest services it can help patients to take the treatment as early as possible.

References

[1] Gorlatova, Maria & Inaltekin, Hazer & Chiang, Mung. (2018). Characterizing Task Completion Latencies in Fog Computing.

[2] Ling, Tonghua & He, Wenchao & Liu, Xianjun & Zhang, Sheng & Huang, Fu & Hua, Fei. (2022). Fine grid model for the dielectric characteristics of ground - penetrating radar in mixed media. Geophysical Prospecting. 70. 10.1111/1365-2478.13214.

[3] Michael, Dennis & Indrajit, Richardus & Dazki, Erick. (2022). Implementation of Enterprise Architecture in Cloud Computing Companies. Sinkron. 7. 549-559. 10.33395/sinkron.v7i2.11407.

[4] Banger, Nanda & K, Pallavi & Shetty, Mrs. (2022). A Review Paper on Cloud Computing Architecture, Types, Advantages and Disadvantages. International Journal of Advanced Research in Science, Communication and Technology. 14-22. 10.48175/IJARSCT-3144.

[5] Ramesh, Varsha & Nair, Siddharth & Tyagi, Amit. (2022). The Fog/Edge Computing: Challenges, Serious Concerns, and the Road Ahead. 10.1002/9781119792437.ch16.

[6] Maloth, Bhav Singh & Anusha, R. & Reddy, R. & Devi, S.Chaya. (2013). Augmentation of Information Security by Cryptography in Cloud Computing. www.ijcst.com. 4.

[7] Deokar, Sanjivani & Mangla, Monika & Akhare, Rakhi. (2021). A Secure Fog Computing Architecture for Continuous Health Monitoring. 10.1007/978-3-030-46197-3_11.

[8 Lin, Rongheng & Ye, Zezhou & Wang, Hao & Wu, Budan. (2018). Chronic Diseases and Health Monitoring Big Data: A Survey. IEEE Reviews in Biomedical Engineering. PP. 1-1. 10.1109/RBME.2018.2829704.

[9] Hamid, Hadeal & Rahman, Sk Md Mizanur & Hossain, M. Shamim & Almogren, Ahmad & Alamri, Atif. (2017). 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. PP. 1-1. 10.1109/ACCESS.2017.2757844.

[10] Kurikala, Geetha & Koppuravuari, Gurnadha & Swapna, A. (2017). Fog Computing : Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology. International Journal of Scientific Research in Computer Science Engineering and Information Technology. 4. 2456-3307.

[11] Vishwanath, Akhilesh & Peruri, Ramya & He, Jing. (2016). Security in Fog Computing through Encryption. International Journal of Information Technology and Computer Science. 8. 28-36. 10.5815/ijitcs.2016.05.03.

[12] Kraemer, Frank & Bråten, Anders & Tamkittikhun, Nattachart & Palma, David. (2017). Fog Computing in Healthcare – A Review and Discussion. IEEE Access. PP. 9206-9222. 10.1109/ACCESS.2017.2704100.

[13] Mouradian, Carla & Naboulsi, Diala & Yangui, Sami & Glitho, Roch & Morrow, Monique & Polakos, Paul. (2017). A Comprehensive Survey on Fog Computing: State-of-the-Art and Research Challenges. IEEE Communications Surveys & Tutorials. PP. 10.1109/COMST.2017.2771153.

[14] Vishwanath, Akhilesh & Peruri, Ramya & He, Jing. (2016). Security in Fog Computing through Encryption. International Journal of Information Technology and Computer Science. 8. 28-36. 10.5815/ijitcs.2016.05.03.

[15] Alexandru, Adriana & Coardos, Dora. (2016). Big Data în Healthcare and Medical Applications in România. Big Data în Healthcare and Medical Applications in România.

[16] Abouelmehdi, Karim & Beni-Hessane, Abderrahim & Khaloufi, Hayat. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data. 5. 10.1186/s40537-017-0110-7.

[17] Geetha Kurikala, K Gurnadha Gupta, A. Swapna.(2017). Fog Computing: Implementation of Security and Privacy to Comprehensive Approach for Avoiding Knowledge Thieving Attack Exploitation Decoy Technology." 2(4).

[18] Malek Ben Salem and Salvatore J. Stolfo(2011). Decoy Document Deployment for Effective Masquerade Attack Detection. 7.

[19] Nisha Peter. (2015). Fog Computing and Its Real Time Applications. International Journal of Emerging Technology and Advanced Engineering, 7.

[20] Mohamed Firdhous, Osman Ghazali and Suhaidi Hassan. "Fog Computing: Will It Be the Future of Cloud Computing?" ISBN: 978-1-941968-00-0, 2014.

[21] Komal Thorat, Shweta Dawkhar, Mansi Kulkarni, Samiksha Wale (2020). Preserving the Privacy of Chronical Big Data Using Fog and Cloud Computing.9(6).

Authors Profile

Mr. Yogesh R. Chikane obtained Bachelor of Engineering degree in Computer Engineering from Savitribai Phule Pune University (M.S.), India, in 2007. Also he received Master of Technology degree in Computer Science and Engineering from RGPV, Bhopal, India in 2013. Currently he is a PhD Research Scholar, Department of Computer Science and Engineering Oriental University, Indore. . He is working as Assistant Professor in Amrutvahini College of Engineering, Sangamner, (M.S.), India. His major area of interest is big data, Machine Learning, AI etc.

Dr. Rashmi Soni,
Research Supervisor and Associate Professor, Department of CSE Oriental University, Indore
Area: big data, Machine Learning, AI etc.

