SECURITY AND CONFIDENTIALITY FOR THE EXCHANGE OF MEDICAL DATA USING CLOUDLETS

INDEX

ABSTRACT

With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing,etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus, in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users'medical data stored in remote cloud of hospital into three parts, and give them properprotection. Finally, in order to protect the healthcare system from malicious attacks, we developa novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, whichcan effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme.

LIST OF FIGURES

LIST OF TABLES

CHAPTER-1

SYSTEM ANALYSIS

1 SYSTEM ANALYSIS

1.1 Existing System:

An MRSE (multi keyword ranked search over encrypted data in cloud computing) privacy protection system was presented, which aims to provide users with a multi-keyword method for the cloud's encrypted data. A priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare date in cloud assisted wireless body area network. The article in the existing system investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare dataaggregation, the security for data processing and misbehavior. The system describes a flexiblesecurity model especially for data centric applications in cloud computing based scenario to make sure data confidentiality, data integrity and fine grained access control to the applicationdata. The system gives a systematic literature review of privacy-protection in cloud-assisted healthcare system.

MRSE (multi-keyword ranked search over encrypted data):

- Multi-keyword ranked search over encrypted data is a technique that allows users to searchfor specific keywords in encrypted data while maintaining the privacy of the data.
- It enables efficient and secure searching over encrypted documents by utilizing cryptographic techniques like symmetric or asymmetric encryption, by which users can retrieve relevant search results without revealing the actual content of the encrypted data.
- It's an interesting approach that combines the benefits of data privacy and search function.

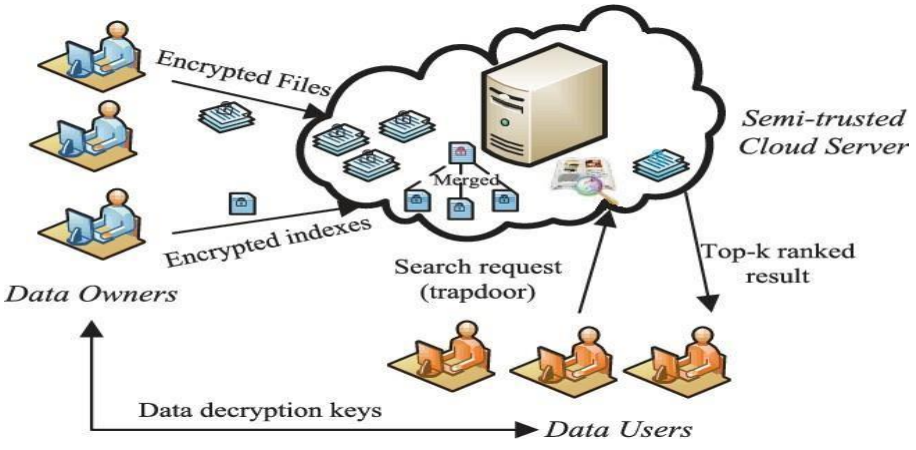


Fig-1 MRSE

1.1.1 Disadvantages of Existing System:

- There is less security on outsourced data due to lack of collaborative intrusion detection system (IDS).
- There is no Remote cloud data privacy protection Scheme.

1.2 Proposed System:

The proposed system, a cloudlet-based +healthcare system is presented, where the privacyof users' physiological data and the efficiency of data transmissions are our main concern. The system uses NTRU for data protection during data transmissions to the cloudlet. In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Basedon the measured users' trust level, the system determines whether data sharing is performed. The proposed system divides data in remote cloud into different kinds and utilizes encryption mechanism to protect them respectively. The Proposed system proposes collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

NTRU (Number Theory Research Unit):

Input: u, v, Message (m).

Output: encrypted and decrypted message.

Step 1: Two small polynomial u and v.

Step 2: The large modulo j and modulo k.

Step 3: The inverse of u modulo k and the inverse of u modulo j.Step 4: u * uk = 1 (mod k) and u * uj= 1 (mod j)

Step 5: Creating uj = u-1 (mod j) and uk = u-1 (mod k).

Step 6: Using j, uk and v, calculate the private key pair and the public key h.

Step 7: h = juk * v (mod k).

Step 8: Encrypted message e is created using m, r and h as follows: e = r * h + m (mod k).

Step 9: The private key u is used to calculate: x = u * e (mod k).

Step 10: z = uj * y (mod j) The polynomial z will be equal to the original message, if decryption procedure has been success full been. successfully finished.

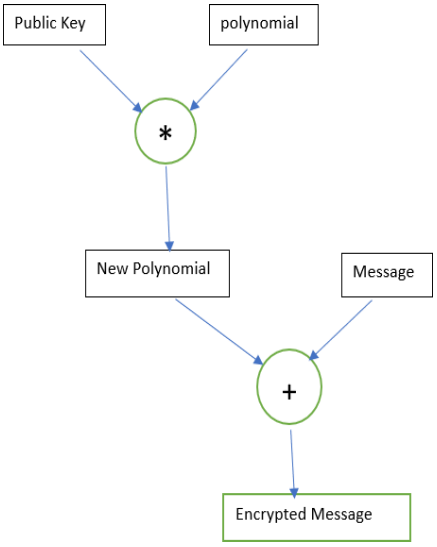


Fig 1.2.1: NTRU ENCRYPTION

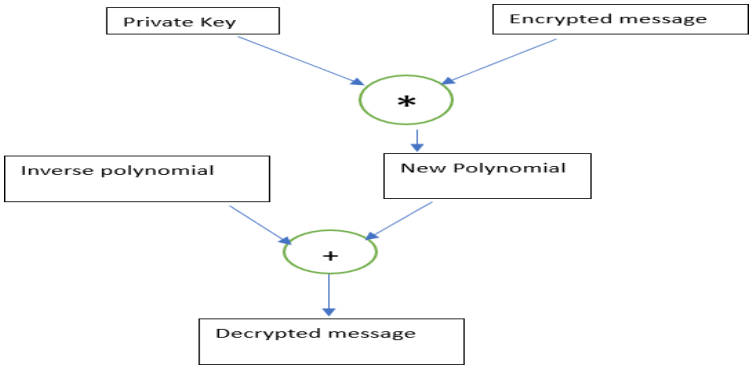


Fig 1.2.2: NTRU DECRYPTION

1.2.1 Advantages of Proposed System:

- The security is more due to Collaboration Intrusion and Detection system.
- Implemented Cloudlet based data sharing which will give more security on out sourced cloud data.

1.3 Introduction:

With the development of healthcare big data and wearable technology, as well as cloud computing and communication technologies, cloud-assisted healthcare big data computing becomes critical to meet users' ever-growing demands on health consultation. However, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion. Previous work suggested the combination of social networks and healthcare service tofacilitate the trace of the disease treatment process for the retrieval of real time disease information. Healthcare social platform, such as Patients- Like Me, can obtain information from other similar patients through data sharing in terms of user's own findings. Though sharing medical data on the social network is beneficial to both patients and doctors, the sensitive data might be leaked or stolen, which causes privacy and security problems without efficient protection for the shared data. Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue.

With the advances in cloud computing, a large amount of data can be stored in various clouds, including cloudlets and remote clouds, facilitating data sharing and intensive computations. However, cloud-based data sharing essentials the following fundamental problems:

• How to protect the security of user's body data during its delivery to a cloudlet?

• How to make sure the data sharing in cloudlet will not cause privacy problem?

• As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?

• How to effectively protect the whole system from malicious attacks?

In terms of the above problems, this paper proposes a cloudlet-based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those dataare further delivered to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, we separate the privacy protection into three stages. In the first stage, user's vital signs collected by wearable devices are delivered to a closet gateway ofcloudlet. During this stage, data privacy is the main concern.

In the second stage, user's data will be further delivered toward remote cloud through cloudlets. A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Especially, we use trust model to evaluate trust level between usersto determine sharing data or not. Considering the users' medical data are stored in remote cloud,we classify these medical data into different kinds and take the corresponding security policy.In addition to above three stages based data privacy protection, we also consider collaborativeIDS based on cloudlet mesh to protect the cloud ecosystem.

In summary, the main contributions of this paper include:

- A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet.
- In order to share data in the cloudlet, we use users' similarity and reputation to build up trustmodel. Based on the measured users' trust level, the system determines whether data sharing is performed.
- We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively.
- We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare systemagainst malic.

CHAPTER-2

LITERATUR SURVEY

2 LITERATURE SURVEY

K. Hung, Y.Zhang,andB.Tai, “Wearable tele home healthcare emergency supplies,"

This paper describes a method that attempts to constantly monitor a patient from indoor or outdoor settings. The device is focus done patient carried Bluetooth PAN, whose central node, a mobile phone, compiles details about the position and health condition of the patient. Such information is secured in order to be transmitted via Wi-fi or GPRS/UMTS to a server. The framework offers facilities for obtaining patient records, including from a J2ME programme from a mobile phone. It also helps the threshold values used to define emergencyconditions to be remotely configured.

M.S.Hossain, "The cyber physical localization framework for patient Monitoring supported by the cloud,"

The promise of cyber-physical systems (CCPSs) enabled by the cloud has attracted a great deal of attention from academia and industry. CCPS s encourage the smooth in corporation with cyber space with technologies in the real environment (e.g. sensors, cameras, microphones, speakers, and GPS devices). This allows for a variety of new technologies or frameworks that enable patient positions to be monitored, such as patient or wellness tracking.A vast range of physical devices, such as sensors with mapping technology (e.g. GPS and cellular local area networks), are built in to these structures to produce, feel, inter pretend exchange massive volumes of medical and user-location data for complicated processing. However, in terms of patient positioning, ubiquitous connectivity, largescale processing, and connectivity, there are arrange of problems with respect to these systems. In terms of immensereal-time data transmission and communications in the cyber or cloud space, there is also a need for an architecture or device that can provide scalability and ubiquity. To this end, this paper proposes a cyber-physical localization framework enabled by the cloud for patient tracking utilising smartphones in a flexible, real-time and effective way to receive voice and electroencephalogram signals. The suggested technique incorporates Gaussian localization mixture simulation and has been shown to outperform other related approaches in terms of error estimation.

J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, A. Streit, J. Kołodziej, and D. "A security framework in g-hadoop for big data computing across distributed cloud datacentres, Georgakopoulos,"

For large-scale data intensive programmes, Map Reduce is known to bean appropriate programming model. The Hadoop architecture is a well-known implementation of Map Reduce that operates the tasks of Map Reduce on a series of clusters. G Hadoop is an expansion of the Hadoop Map Reduce architecture with the potential to allow Map Reduce tasks in a Grid system to operate on several clusters. G-Hadoop, however, merely reuses Hadoop's user authentication and work submission system, which is intended for a single cluster and is therefore not appropriate for the Grid context. A new protection paradigm for G-Hadoop is being proposed in this work. The protection paradigm is focused on many security solutions and is primarily developed for distributed systems such as the Grid, such as public key cryptography and the SSL protocol. This protection architecture simplifies the method of authenticating users and uploading jobs with a single-sign-on solution to the existing G- Hadoop implementation. In

addition, a range of different protection frameworks are included in the built security frame work to defend the G-Hadoop system against conventional attacks as well as exploitation and misuse.

M. Around S. Hossain and G. 'Cloud-assisted industrial internet of things (iiot)-enabled health surveillance system,' Muhammad,

In the next-generation healthcare sector for better patient treatment, the exciting promiseof the new Internet of Things (IoT) technology for integrated medical equipment and sensors has played an important role. Because of the growing number of aged and disabled persons, there is an immediate need for an infrastructure for real-time clinical surveillance to analyze health data from patients and prevent preventable deaths. Healthcare Industrial IoT (Health IIoT) has considerable scope for such surveillance to be carried out. Health IIoT is a mix of networking systems, integrated software, things (devices and sensors) and entities that operatetogether as a single smart frame work to control, track and store health information for continuing treatment for patients. This paper introduces a tracking system allowed by Health IIoT, where ECG and other healthcare data are captured by mobile devices and sensors and safely transmitted to the cloud for healthcare practitioners to provide seamless access. To deterdata fraud or clinical negligence by healthcare practitioners, signal optimization, watermarking, and other associated analytics can be utilized.

L. Griffin and E. De Leastar, "Social networking healthcare," in Wearable Micro and Nano Technologies for PersonalizedHealth"

State of the art and future challenges. The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise. The proposed work also attempts to minimize the end-to-end packet delay by choosing dynamically a neighbour cloudlet, so that the overall delay is minimized. Privacy-preserving multi-keyword ranked search over encrypted cloud data. We first offer a basic idea for the multi keyword ranked search over encrypted cloud data (MRSE) based on effective comparison measure of coordinate matching. A collaborative intrusion detection and prevention system in cloud computing. We propose a collaborative model consists of the Intrusion Detection and Prevention System functions based distributed IDS and IPS, with the use of a hybrid detection technique for addressing the problems of attacks encountered, specifically distributed attacks such as port scanning attacks and distributed internally established within a Cloud Computing environment by users entitled to access, including the integration of the Signature A priori Algorithm for generating new attack signatures whose objective is to develop the functioning of our security system to be able to detect and block various types of attacks and intrusions. Security models and requirements for healthcare application clouds. We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud.

CHAPTER-3
SYSTEM DESIGN

3 SYSTEM DESIGN

3.1 SYSTEM ARCHITECTURE

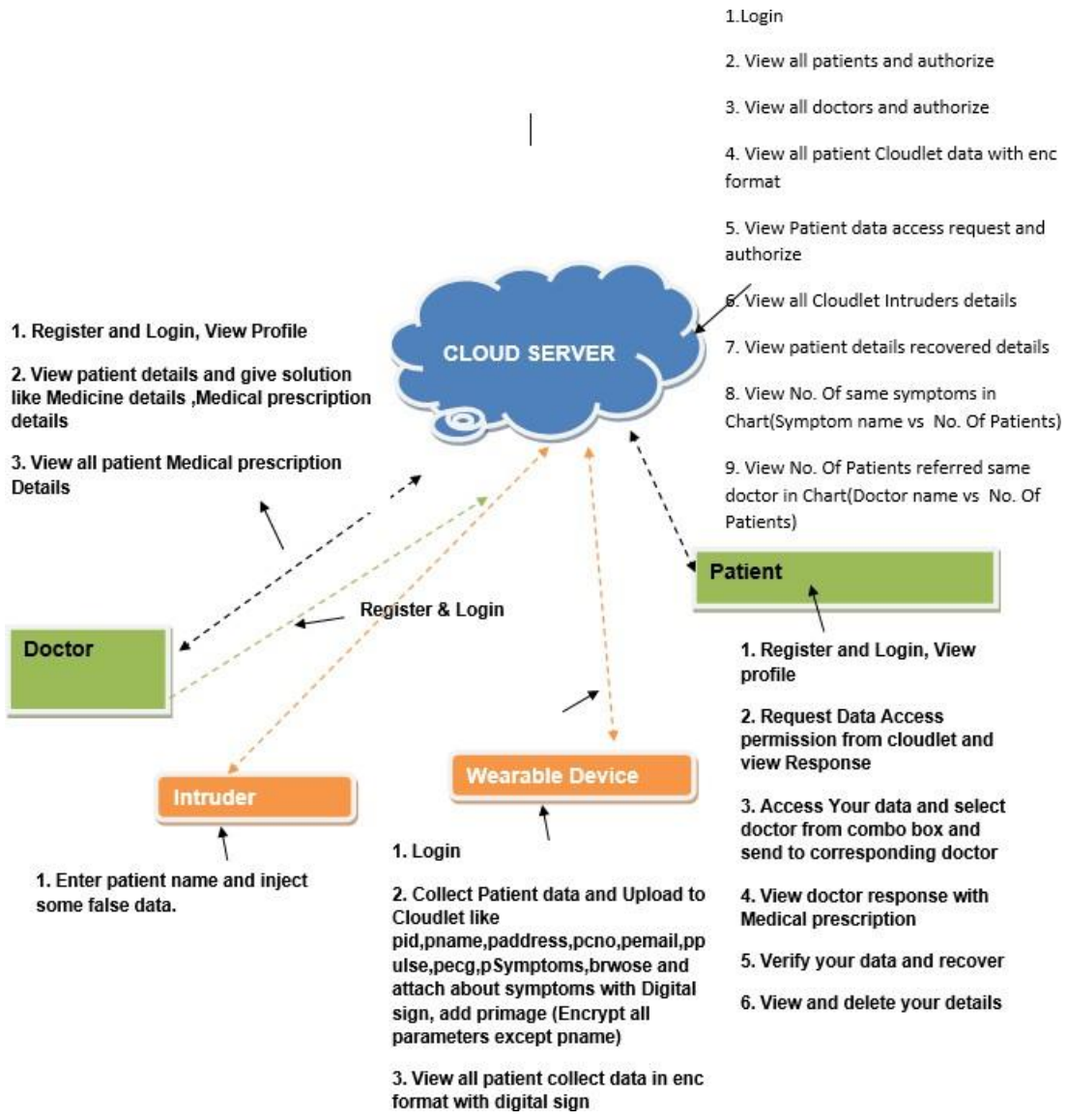


Fig 3.1 System Architecture

3.1.1 MODULES

- **Wearable Device**

In this module, the wearable device Collect Patient data and Upload to Cloudlet like pid,pname,paddress,pcno,pemail,ppulse,pecg,pSymptoms, browse and attach about symptoms with Digital sign, add pimage(Encrypt all parameters except pname) and view all patient collect data in enc format with digital sign.

- **Cloud Server**

The **Cloud** server manages which is to provide data storage service for the wearable devices and also View all patients and authorize and view all doctors and authorize, view all patient Cloudlet data with enc format, View Patient data access request and authorize, view all Cloudlet Intruders details and View patient details recovered details, View No. Of same symptoms in Chart (Symptom name vs No. Of Patients), View No. Of Patients referred same doctor in Chart (Doctor name vs No. Of Patients).

- **Patient**

In this module, the patient Register and Login, View profile, Request Data Access permission from cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with medical prescription, verify yourdata and recover and view and delete your details.

- **Doctor**

The doctor is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, medical prescription details View all patient medical prescription Details.

3.1.2 UML DIAGRAMS

3.1.2.1 USE CASE DIAGRAM

Cloud Server:

The **Cloud Server** manages which is to provide data storage service for the wearable devices and also View all patients and authorize and view all doctors and authorize, view all patient Cloudlet data with enc format, View Patient data access request and authorize, view all Cloudlet Intruders details and View patient details recovered details, View No. Of same symptoms in Chart (Symptom name vs No. Of Patients), View No. Of Patients referred same doctor in Chart (Doctor name vs No. Of Patients).

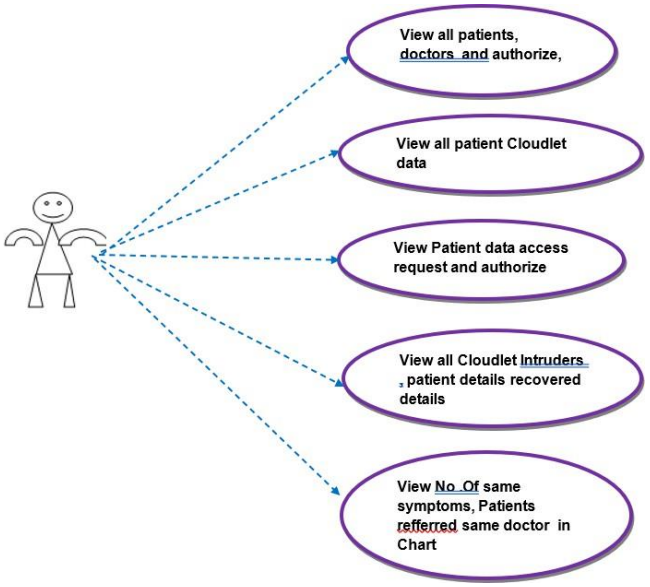


Fig-3.1.2.1a Cloud Server

Patient:

The patient Register and Login, View profile, Request Data Access permissionfrom cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with medical prescription, verify yourdata and recover and view and delete your details.

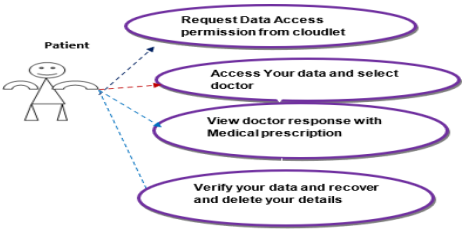


Fig-3.1.2.1b Patient

Doctor:

The doctor is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, medical prescription details View all patient medical prescription Details.

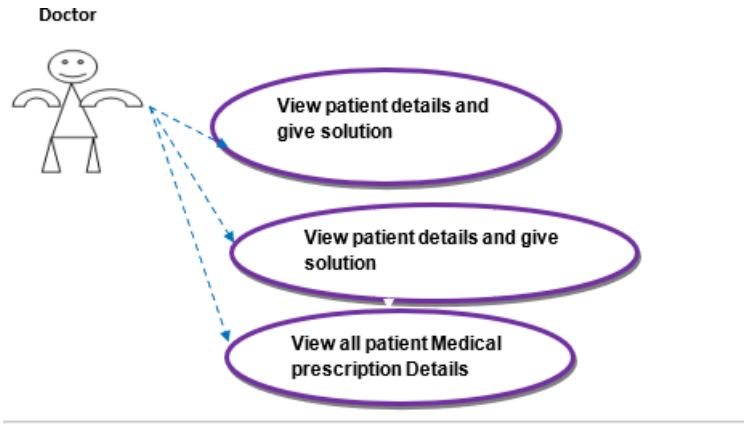


Fig-3.1.2.1c Doctor

Wearable Device:

The wearable device Collect Patient data and Upload to Cloudlet like pid,pname,paddress,pcno,pemail,ppulse,pecg,pSymptoms, browse and attach about symptoms with Digital sign, add pimage(Encrypt all parameters except pname) and view all patient collect data in enc format with digital sign.

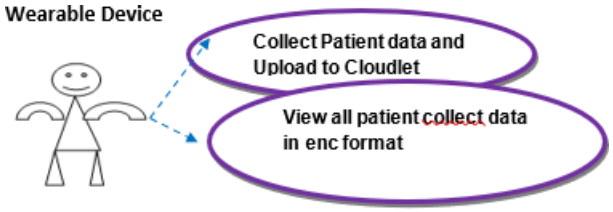


Fig-3.1.2.1d Wearable Device

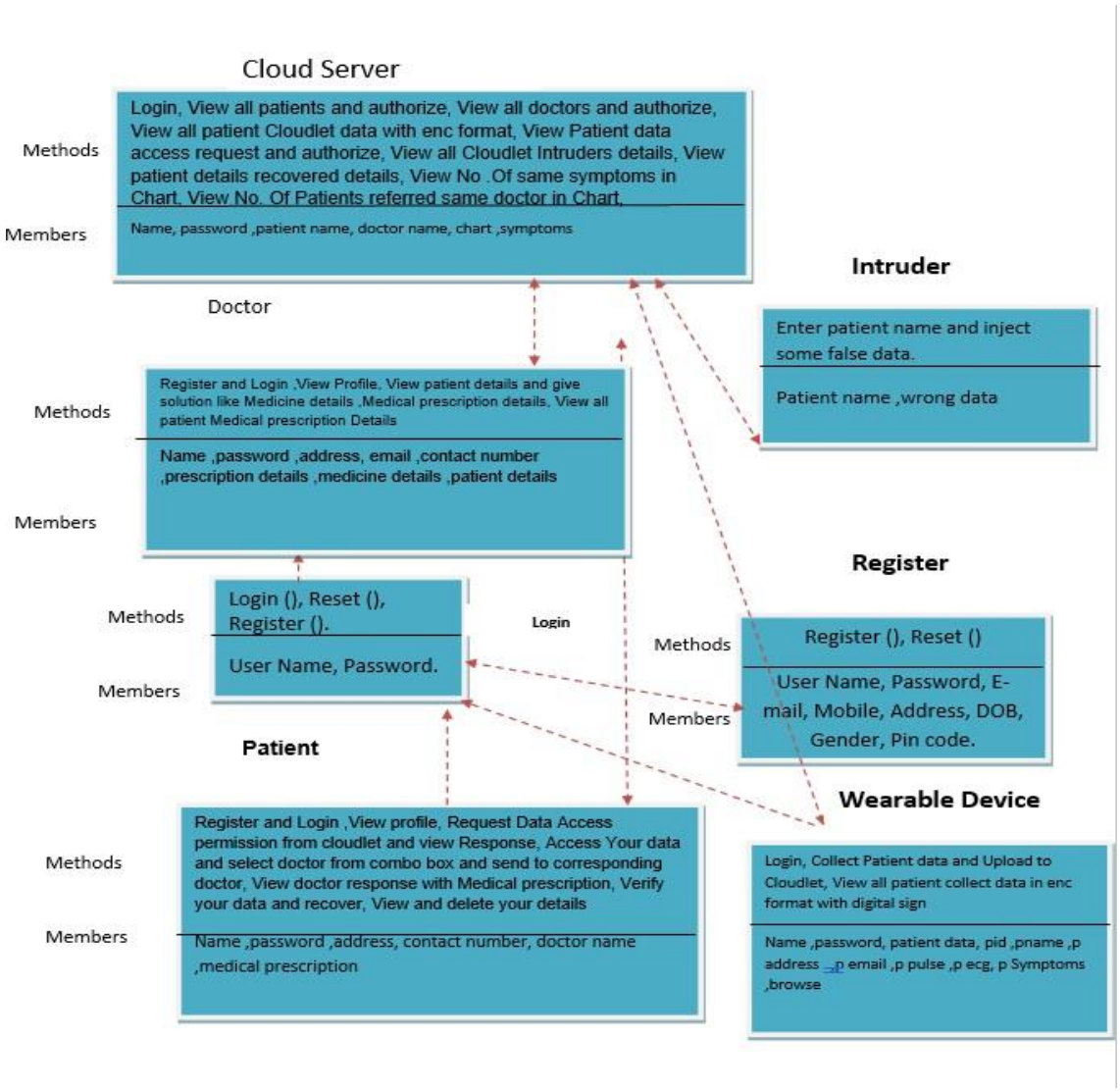
Intruder:

The intruder will collect the patient data and inject some false data in order to change the original data of the patient.

Fig-3.1.2.1e Intruder

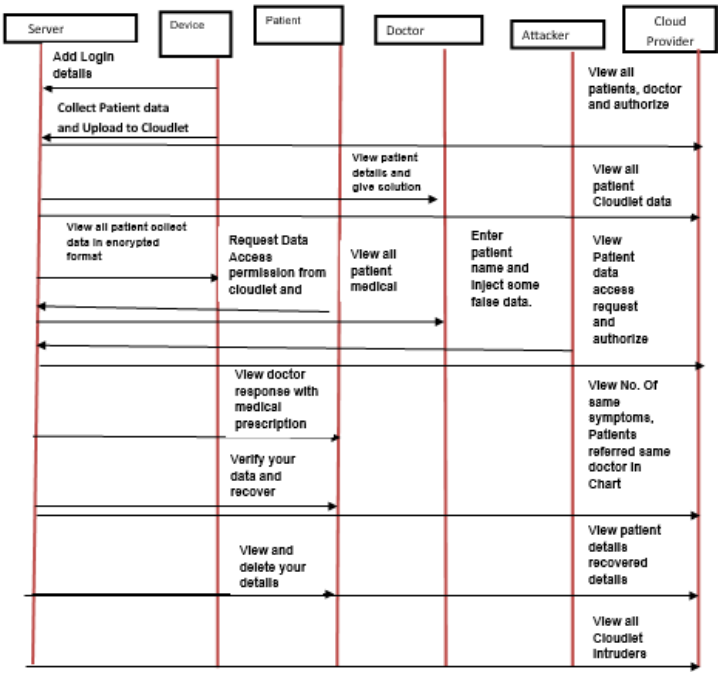
3.1.2.2 CLASS DIAGRAM

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.



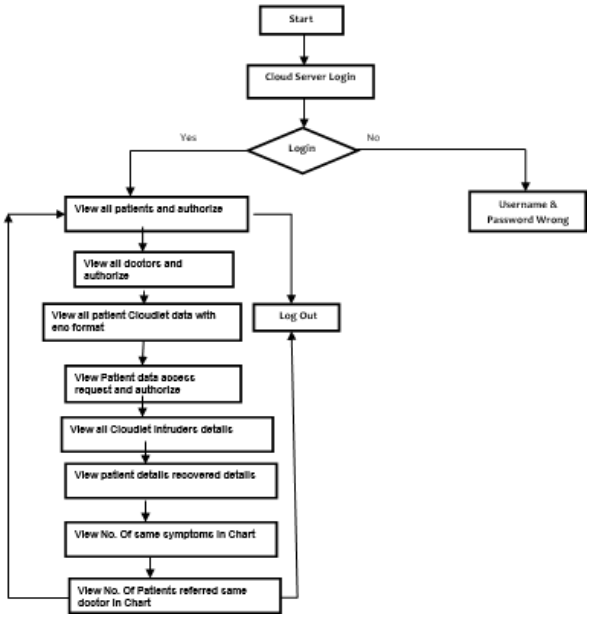
3.1.2.3 SEQUENCE DIAGRAM:

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart.



3.1.2.4 ACTIVITY DIAGRAM:

Activity diagram is another important behavioral diagram in UML diagram to describe dynamic aspects of the system. Activity diagram is essentially an advanced version of flow chart that modeling the flow from one activity to another activity.



3.2 SYSTEM REQUIREMENTS:

3.2.1 Hardware Requirements:

System	11thGen Intel(R) Core (TM)i5-1135G7 @2.40GHz
Hard Disk	1TB
Ram	8 GB
Monitor	15.6 HD WVA Display

3.2.2 Software Requirements:

Operating system	Windows 11
Coding Language	Java

CHAPTER-4

INPUT AND OUTPUT DESIGN

4 INPUT AND OUTPUT DESIGN

4.1 Input Design:

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So, inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and otherrelated validations. This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the rightway so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided with in an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

4.2 Output Design:

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members,in other words, the administrator and the clients. The output of VPN is the system which allowsthe project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level accessto each client on the user side depending on the projects allotted to him. After completion of aproject, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new user rest with the administrator only.

The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

CHAPTER5

SYSTEM ENVIRONMENT

5 SYSTEM ENVIRONMENT

5.1 Java Technology

Java technology is both a programming language and a platform.

Java is a programming language and computing platform first released by Sun Microsystems in 1995. It has evolved from humble beginnings to power a large share of today's digital world,by providing the reliable platform upon which many services and applications are built. New, innovative products and digital services designed for the future continue to rely on Java, as well.

While most modern Java applications combine the Java runtime and application together, thereare still many applications and even some websites that will not function unless you have a desktop Java installed. Java.com, this website, is intended for consumers who may still requireJava for their desktop applications.

The Java Programming Language

The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

- Simple
- Object oriented
- Distributed
- Multithreaded
- Dynamic
- Architecture neutral
- Portable
- High performance
- Robust
- Secure

Each of the preceding buzzwords is explained in The Java Language Environment , a white paper written by James Gosling and Henry McGilton.

In the Java programming language, all source code is first written in plain text files ending withthe .java extension. Those source files are then compiled into .class files by the javac compiler. A .class file does not contain code that is native to your processor; it instead contains bytecodes — the machine language of the Java Virtual Machine[1] (Java VM). The java launcher tool then runs your application with an instance of the Java Virtual Machine.

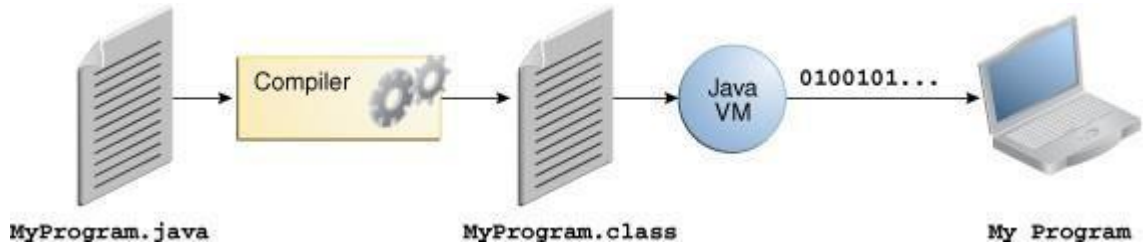


Fig 5.1.1a An overview of the software development process.

Because the Java VM is available on many different operating systems, the same .class files are capable of running on Microsoft Windows, the Solaris™ Operating System (Solaris OS), Linux, or Mac OS. Some virtual machines, such as the Java SE HotSpot at a Glance, perform additional steps at runtime to give your application a performance boost. This includes varioustasks such as finding performance bottlenecks and recompiling (to native code) frequently usedsections of code.

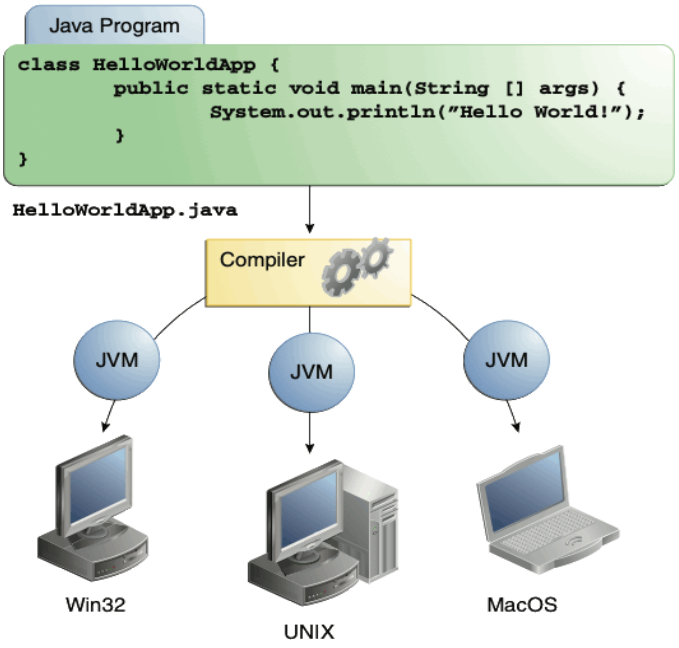


Fig 5.1.b Java

Through the Java VM, the same application is capable of running on multiple platforms.

5.1.1 History of Java

Initially the language was called as "oak" but it was renamed as "Java" in 1995. The primary motivation of this language was the need for a platform-independent (i.e., architectureneutral) language that could be used to create software to be embedded in various consumer electronic devices.

- Java is a programmer's language.
- Java is cohesive and consistent.
- Except for those constraints imposed by the Internet environment, Java gives the programmer,full control.

Finally, Java is to Internet programming where C was to system programming.

5.1.2. What can Java do?

Java has had a profound effect on the Internet. This is because; Java expands the Universeof objects that can move about freely in Cyberspace. In a network, two categories of objects are transmitted between the Server and the Personal computer. They are: Passive information and Dynamic active programs. The Dynamic, Self-executing programs cause serious problemsin the areas of Security and probability.

5.1.3 Why Java?

Java can be used to create two types of programs:

Applications and Applets: An application is a program that runs on our Computer under the operating system of that computer. It is more or less like one creating using C or C++. Java's ability to create Applets makes it important. An Applet is an application designedto be transmitted over the Internet and executed by a Java –compatible web browser. An applet is actually a tiny Java program, dynamically downloaded across the network, just like an image.But the difference is, it is an intelligent program, not just a media file. It can react to the user input and dynamically change.

5.1.4 Java syntax compared to other languages:

The key that allows the Java to solve the security and portability problems is that the outputof Java compiler is Byte code. Byte code is a highly optimized set of instructions designed to be executed by the Java run-time system, which is called the Java Virtual Machine (JVM). Thatis, in its standard form, the JVM is an interpreter for byte code.

Java Virtual Machine (JVM):

Beyond the language, there is the Java virtual machine. The Java virtual machine is an important element of the Java technology. The virtual machine can be embedded within a web browser or an operating system. Once a piece of Java code is loaded onto a machine, it is verified. As part of the loading process, a class loader is invoked and does byte code verificationmakes sure that the code that's has been generated by the compiler will not corrupt the machinethat it's loaded on. Byte code verification takes place at the end of the compilation process to make sure that is all accurate and correct. So byte code verification is integral to the compilingand executing of Java code.

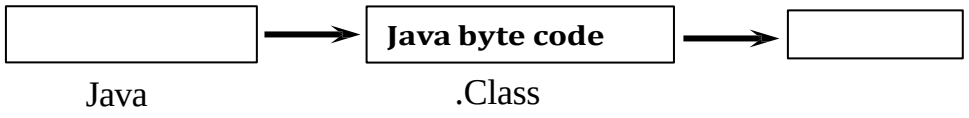


Fig 5.1.4a Picture showing the development process of JAVA Program

Java programming uses to produce byte codes and executes them. The first box indicates that the Java source code is located in a. Java file that is processed with a Java compiler calledjava c. The Java compiler produces a file called a. class file, which contains the byte code. The.Class file is then loaded across the network or loaded locally on your machine into the execution environment is the Java virtual machine, which interprets and executes the byte code.

Java Architecture:

Java architecture provides a portable, robust, high performing environment for development. Java provides portability by compiling the byte codes for the Java Virtual Machine, which is then interpreted on each platform by the run-time environment. Java is a dynamic system, able to load code when needed from a machine in the same room or across the planet.

Compilation of code:

When you compile the code, the Java compiler creates machine code (called byte code) for a hypothetical machine called Java Virtual Machine (JVM). The JVM is supposed to execute the byte code. The JVM is created for overcoming the issue of portability. The code iswritten and compiled for one machine and interpreted on all machines. This machine is calledJava Virtual Machine.

Compiling and interpreting Java Source Code:

During run-time the Java interpreter tricks the byte code file into thinking that it is runningon a Java Virtual Machine. In reality this could be a Intel Pentium Windows 95 or Sun SARC

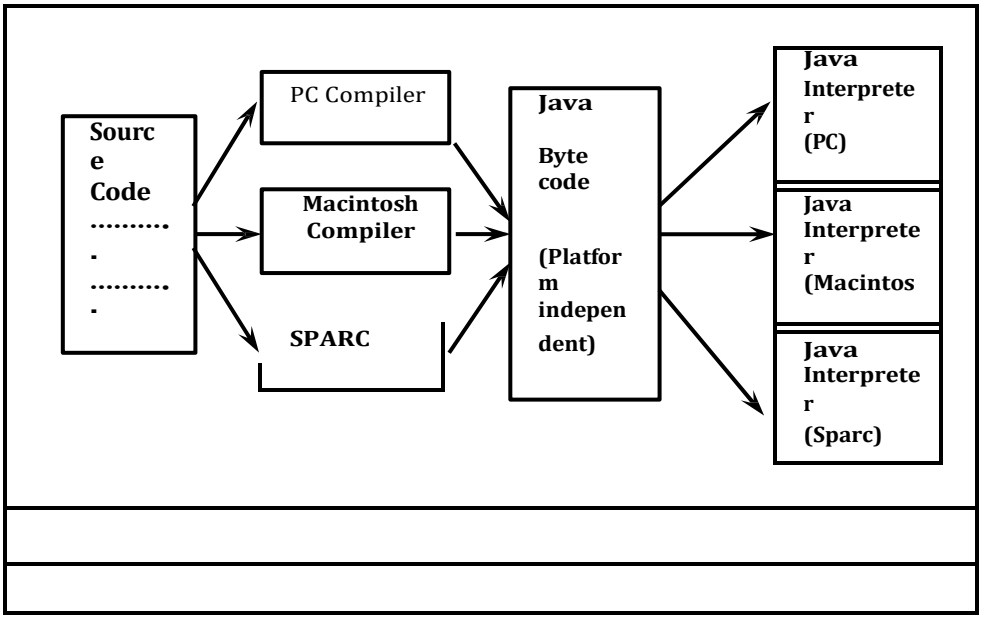


Fig 5.1.4b Java Compiling

station running Solaris or Apple Macintosh running system and all could receive code from any computer through Internet and run the Applets.

5.1.5 Uses of java:

In comparison to other programming languages, Java stands alone for its security and functionality. Java isolates itself from other programming languages because of functionality and security and it is relevant too. There are some other reasons to use Java are as follows:

- **Scalability:** Scalability adds capacity to our system. It improves the capacity of the system by adding the system resources without affecting the deployment architecture. Wecan achieve scalability by increasing the resources such as RAM and CPU in a single system. It is important because it handles the workload, increases the system performance,and maximizes productivity.
- **Cross-Platform:** Cross-platform means, a compiled Java program can be run on all the platforms. Remember that the system must have JVM. After compiling a Java program, the Java code gets converted into the bytecode which is platform-independent. This bytecode is understood by the JVM. We can run this bytecode on any platform.
- **Memory-Management:** Java provides its own mechanism for managing the memoryis known as garbage collection. We need not to care about memory and do not require to implement it to manage the memory. It automatically deletes the objects when they no longer used by the application. It improves the speed of the application.
- **Multi-threading:** Thread is a light-weight subprocess. Multi-threading in Java allows concurrent execution of two or more threads simultaneously. It maximizes the utilization of the CPU.

5.1.6 Features of Java:

Security:

Every time you that you download a “normal” program, you are risking a viral infection. Prior to Java, most users did not download executable programs frequently, and those who did scanned them for viruses prior to execution. Most users still worried about the possibility of infecting their systems with a virus. In addition, another type of malicious program exists that must be guarded against. This type of program can gather private information, such as credit card numbers, bank account balances, and passwords. Java answers both these concerns by providing a “firewall” between a network application and your computer.

When you use a Java-compatible Web browser, you can safely download Java applets without fear of virus infection or malicious intent.

Portability:

For programs to be dynamically downloaded to all the various types of platforms connected to the Internet, some means of generating portable executable code is needed . As you will see, the same mechanism that helps ensure security also helps create portability.

Simple:

Java was designed to be easy for the Professional programmer to learn and to use effectively. If you are an experienced C++ programmer, learning Java will be even easier. Because Java inherits the C/C++ syntax and many of the object oriented features of C++. Mostof the confusing concepts from C++ are either left out of Java or implemented in a cleaner, more approachable manner. In Java there are a small number of clearly defined ways to accomplish a given task.

Object-Oriented:

Java was not designed to be source-code compatible with any other language. This allowedthe Java team the freedom to design with a blank slate. One outcome of this was a clean usable, pragmatic approach to objects. The object model in Java is simple and easy to extend, while simple types, such as integers, are kept as high-performance non-objects.

Robust:

The multi-platform environment of the Web places extraordinary demands on a program, because the program must execute reliably in a variety of systems. The ability to create robust programs was given a high priority in the design of Java. Java is strictly typed language; it checks your code at compile time and run time.

Java virtually eliminates the problems of memory management and deallocation, which is completely automatic. In a well-written Java program, all run time errors can –and should –be managed by your program.

5.2 JAVASCRIPT:

JavaScript is a script-based programming language that was developed by Netscape Communication Corporation. JavaScript was originally called Live Script and renamed as JavaScript to indicate its relationship with Java. JavaScript supports the development of both client and server components of Web-based applications. On the client side, it can be used to write programs that are executed by a Web browser within the context of a Web page. On the server side, it can be used to write Web server programs that can process information submittedby a Web browser and then updates the browser's display accordingly.

<SCRIPTS>..</SCRIPT>.

<SCRIPT LANGUAGE = "JavaScript">

JavaScript statements

</SCRIPT>

5.2.1 Java script vs java:

JavaScript and Java are entirely different languages. A few of the most glaring differences are:

- Java applets are generally displayed in a box within the web document; JavaScript can affect any part of the Web document itself.
- While JavaScript is best suited to simple applications and adding interactive features to Webpages. Java can be used for incredibly complex applications.

5.3 Java Database Connectivity:

What Is JDBC?

JDBC is a Java API for executing SQL statements. (As a point of interest, JDBC is a trademarked name and is not an acronym; nevertheless, JDBC is often thought of as standing for Java Database Connectivity. It consists of a set of classes and interfaces written in the Java programming language. JDBC provides a standard API for tool/database developers and makesit possible to write database applications using a pure Java API. Using JDBC, it is easy to sendSQL statements to virtually any relational database. One can write a single program using theJDBC API, and the program will be able to send SQL statements to the appropriate database. The combinations of Java and JDBC lets a programmer write it once and run it anywhere.

What Does JDBC Do?

Simply put, JDBC makes it possible to do three things:

- Establish a connection with a database
- Send SQL statements
- Process the results.

5.4 Java Server Pages (JSP):

Java Server Pages is a simple, yet powerful technology for creating and maintaining dynamic-content web pages. Based on the Java programming language, Java Server Pages offers proven portability, open standards, and a mature re-usable component model. The Java Server Pages architecture enables the separation of content generation from content presentation. This separation not eases maintenance headaches, it also allows web teammembers to focus on their areas of expertise. Now, web page designer can concentrate on layout, and web application designers on programming, with minimal concern about impactingeach other's work.

5.4.1 Features of JSP:

Portability:

Java Server Pages files can be run on any web server or web-enabled application server that provides support for them. Dubbed the JSP engine, this support involves recognition, translation, and management of the Java Server Page lifecycle and its interaction components.

Components:

It was mentioned earlier that the Java Server Pages architecture can include reusable Java components. The architecture also allows for the embedding of a scripting language directly into the Java Server Pages file. The components current supported include Java Beans, and Servlets.

Processing:

A Java Server Pages file is essentially an HTML document with JSP scripting or tags. The Java Server Pages file has a JSP extension to the server as a Java Server Pages file. Before the page is served, the Java Server Pages syntax is parsed and processed into a Servlet on the server side. The Servlet that is generated outputs real content in straight HTML for responding to the client.

Access Models:

A Java Server Pages file may be accessed in at least two different ways. A client's request comes directly into a Java Server Page. In this scenario, suppose the page accesses reusable Java Bean components that perform particular well-defined computations like accessing a database. The result of the Beans computations, called result sets is stored within the Bean as properties. The page uses such Beans to generate dynamic content and present it back to the client.

In both of the above cases, the page could also contain any valid Java code. Java Server Pages architecture encourages separation of content from presentation.

Steps in the execution of a JSP Application:

1. The client sends a request to the web server for a JSP file by giving the name of the JSPfile within the form tag of a HTML page.
2. This request is transferred to the Java Web Server. At the server side Java Web Server receives the request and if it is a request for a jsp file server gives this request to the JSP engine.
3. JSP engine is program which can understands the tags of the jsp and then it converts those tags into a Servlet program and it is stored at the server side. This Servlet is loaded in the memory and then it is executed and the result is given back to the Java Web Server and then it is transferred back to the result is given back to the Java Web Server and then it is transferred back to the client.

JDBC connectivity:

The JDBC provides database-independent connectivity between the J2EE platform and a wide range of tabular data sources. JDBC technology allows an Application Component Provider to:

- Perform connection and authentication to a database server
- Manager transactions
- Move SQL statements to a database engine for preprocessing and execution
- Execute stored procedures
- Inspect and modify the results from Select statements.

5.5 Tomcat 6.0 web server:

Tomcat is an open source web server developed by Apache Group. Apache Tomcat is the servlet container that is used in the official Reference Implementation for the Java Servlet and Java Server Pages technologies. The Java Servlet and Java Server Pages specifications are developed by Sun under the Java Community Process. Web Servers like Apache Tomcat support only web components while an application server supports web components as well asbusiness components (BEAs Web logic, is one of the popular application server).To develop a web application with jsp/servlet install any web server like J Run, Tomcat etc to run your application.

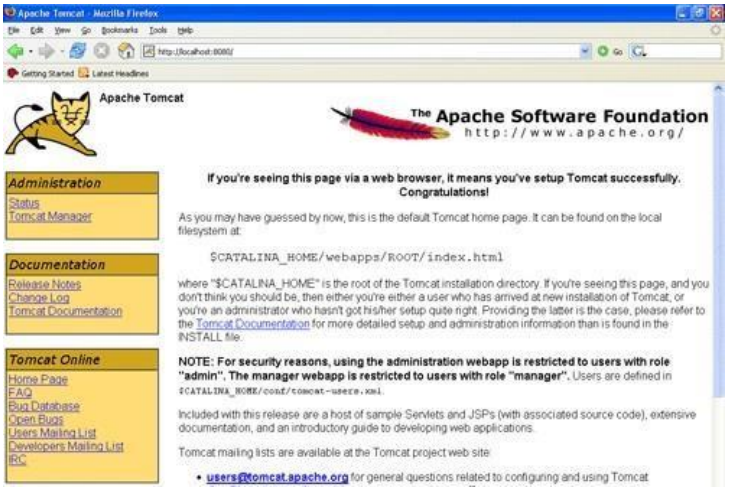


Fig5.6.a Tomcat Webserver

CHAPTER-6

SYSTEM STUDY

6 SYSTEM STUDY

FEASIBILITY STUDY:

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

- **Economic Feasibility**
- **Technical Feasibility**
- **Operational Feasibility**.

6.1 Economic Feasibility:

Economic Feasibility or Cost-benefit is an assessment of the economic justification fora computer based project. As hardware was installed from the beginning & for lots of purposesthus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at any time.The Virtual Private Network is to be developed using the existing resources of the organization.So, the project is economically feasible.

6.2 Technical Feasibility:

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existingfacility.

6.3 Operational Feasibility:

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the admin and helps him in effectivelytracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible

CHAPTER-7
SYSTEM TESTING

7 SYSTEM TESTING

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of tests. Each test type addresses a specific testing requirement.

Software once validated must be combined with other system elements (e.g. Hardware, people, database). System testing verifies that all the elements are proper and that overall system function performance is achieved. It also tests to find discrepancies between the system and its original objective, current specifications and system documentation.

7.1 TYPES OF TESTS:

7.1.1 Unit Testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program inputs produce valid outputs. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accuratelyto the documented specifications and contains clearly defined inputs and expected results.

7.1.2 Integration Testing:

Integration testing addresses the issues associated with the dual problems of verification and program construction. After the software has been integrated a set of high order tests are conducted. The main objective in this testing process is to take unit tested modules and buildsa program structure that has been dictated by design.

The following are the types of Integration Testing:

1. Top Down Integration

This method is an incremental approach to the construction of program structure. Modulesare integrated by moving downward through the control hierarchy, beginning with the main program module. The module subordinates to the main program module are incorporated intothe structure in either a depth first or breadth first manner.

1. Bottom-up Integration

This method begins the construction and testing with the modules at the lowest level in the program structure. Since the modules are integrated from the bottom up, processing required for modules subordinate to a given level is always available and the need for stubs is eliminated.

The bottom up integration strategy may be implemented with the following steps:

- The low-level modules are combined into clusters into clusters that perform a specificSoftware sub-function.
- A driver (i.e.) the control program for testing is written to coordinate test case input andoutput.
- The cluster is tested.
- Drivers are removed and clusters are combined moving upward in the program structure

The bottom-up approaches test each module individually and then each module is module is integrated with a main module and tested for functionality.

7.1.3 Functional test:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input	: identified classes of valid input must be accepted.
Invalid Input	: identified classes of invalid input must be rejected.
Functions	: identified functions must be exercised.
Output	: identified classes of application outputs must be exercised.
Systems/Procedures	: interfacing systems or procedures must be invoked.

Organization and preparation of functional tests is focused on requirements, key functions,or special test cases. In addition, systematic coverage pertaining to identify Business process flows; data fields, predefined processes, and successive processes must be considered for testing. Before functional testing is complete, additional tests are identified and the effective value of current tests is determined.

7.1.4 System Test

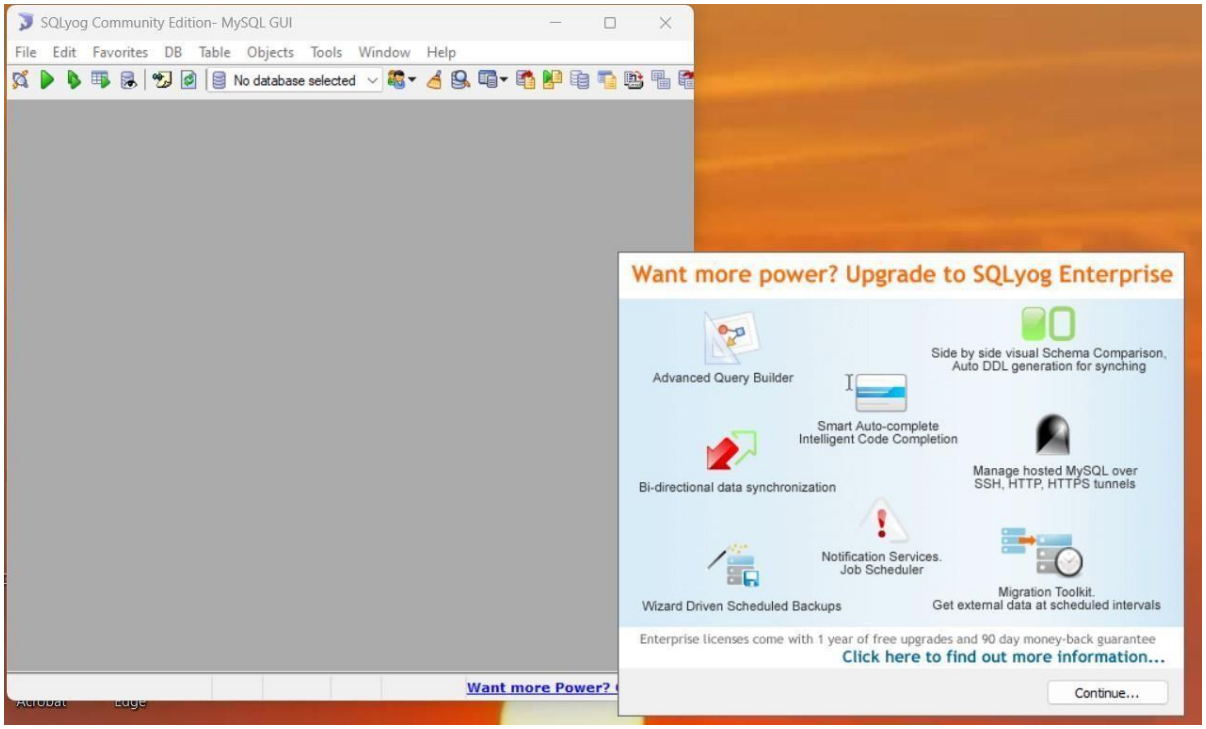
System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing isthe configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

7.1.5 Acceptance Testing:

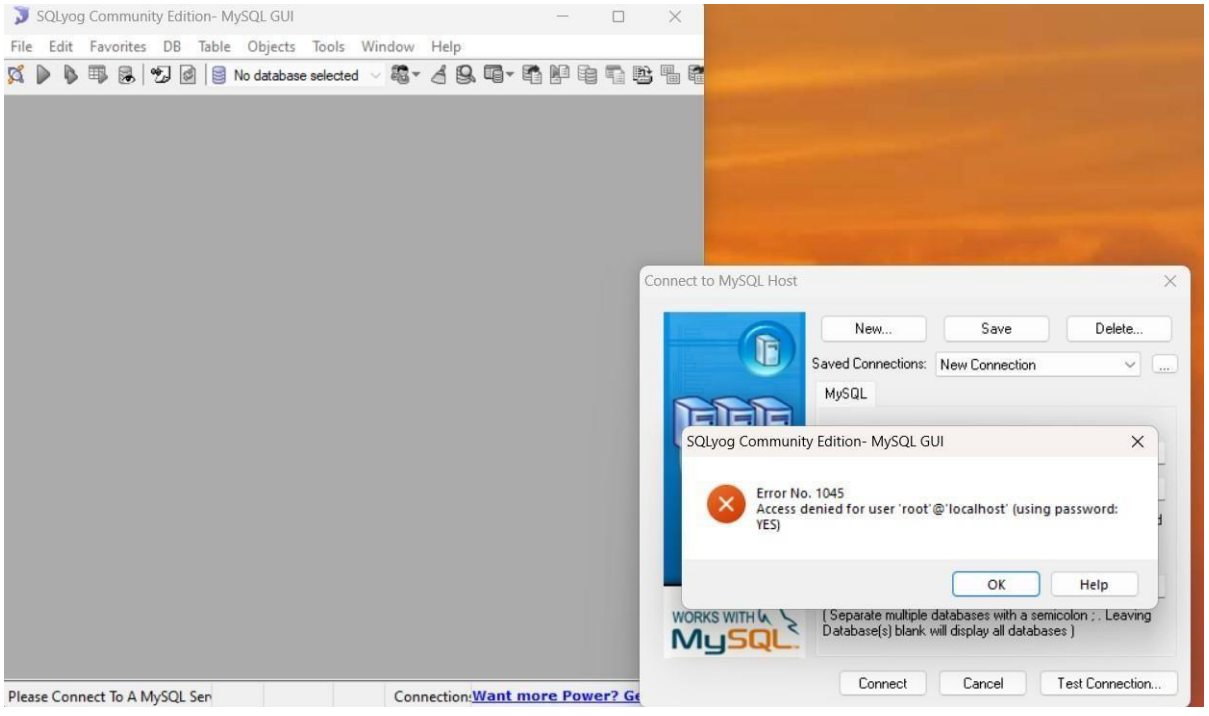
User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

7.1.6 Test Cases:

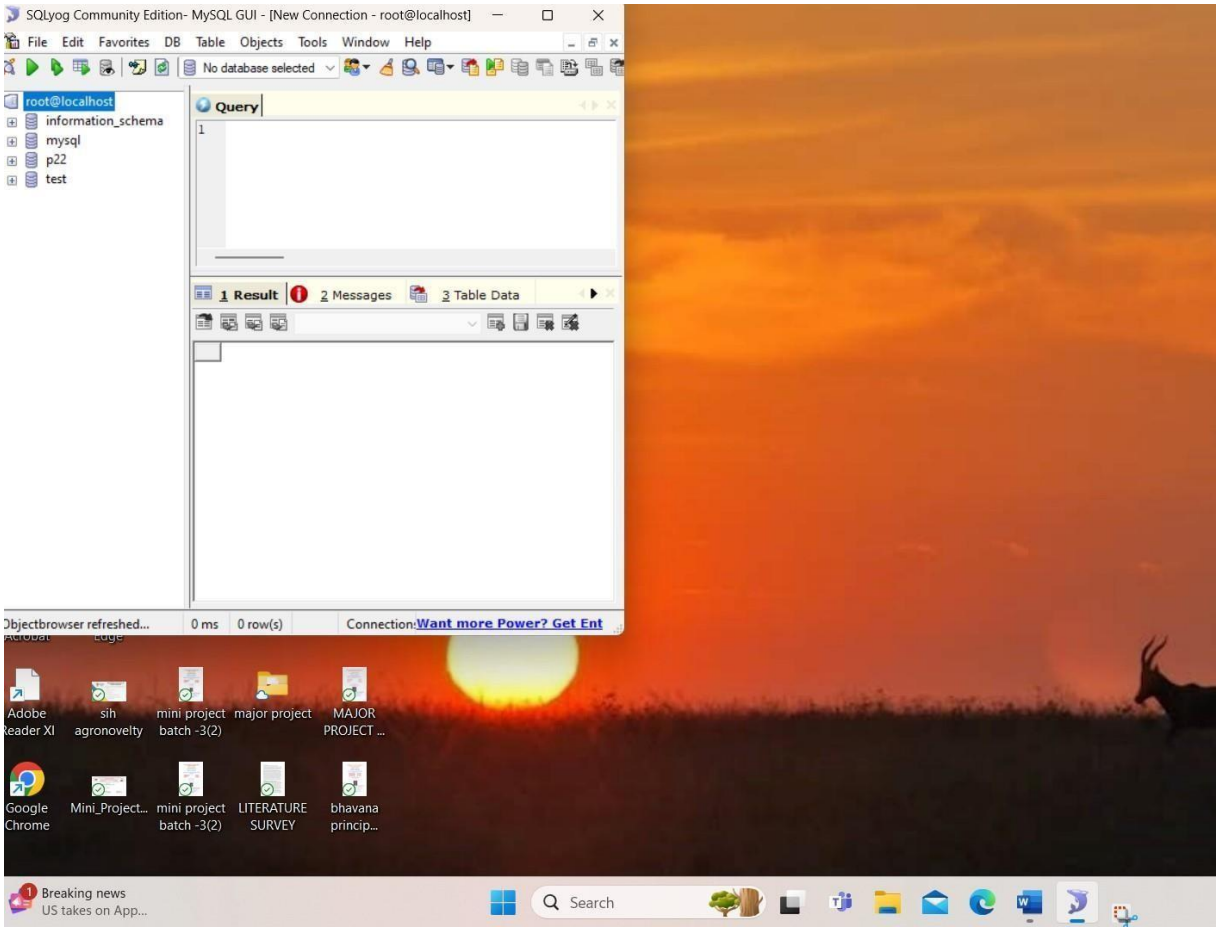
Test Case-1:



open the sqlyog in order to access the dataset

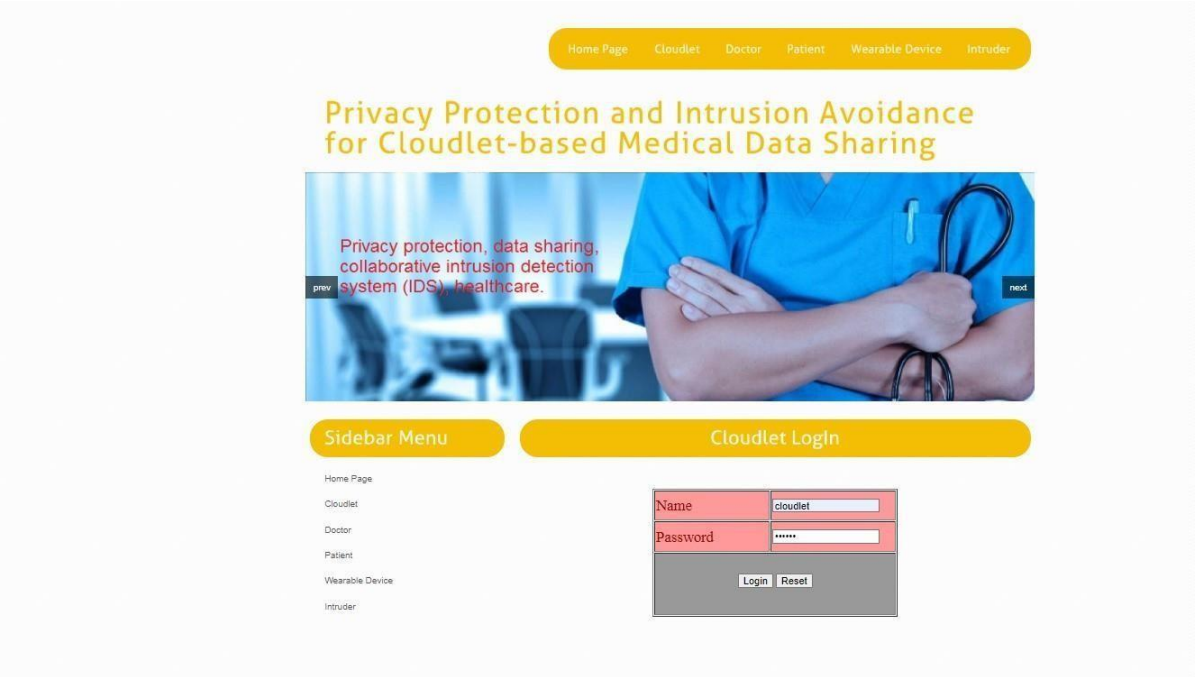


The access denied due to wrong user had entered

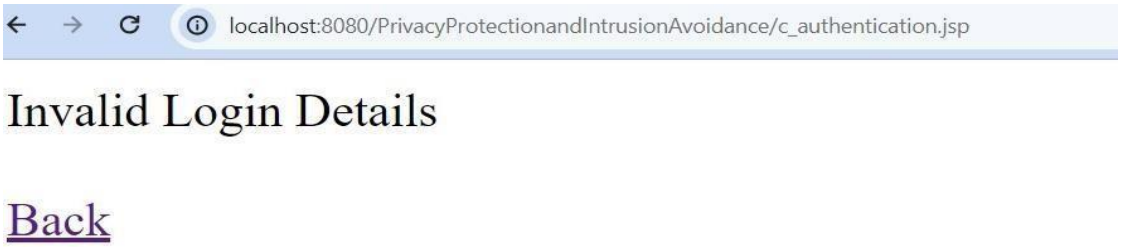


The user was successfully entered into the database

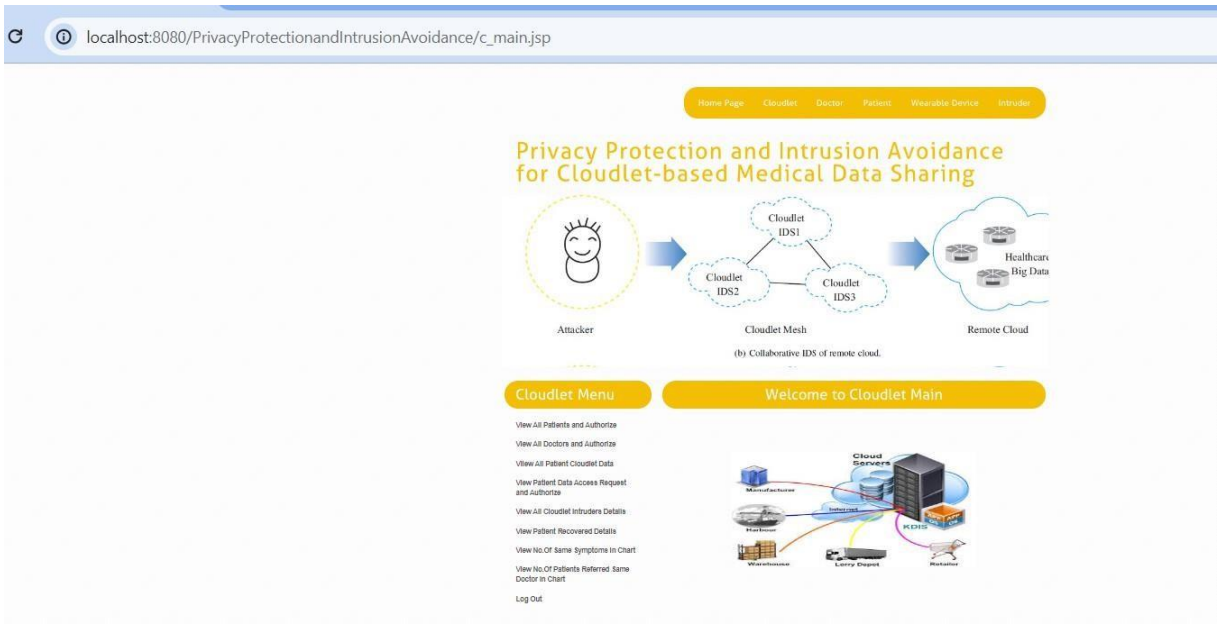
Test Case-2



Cloudlet details are given

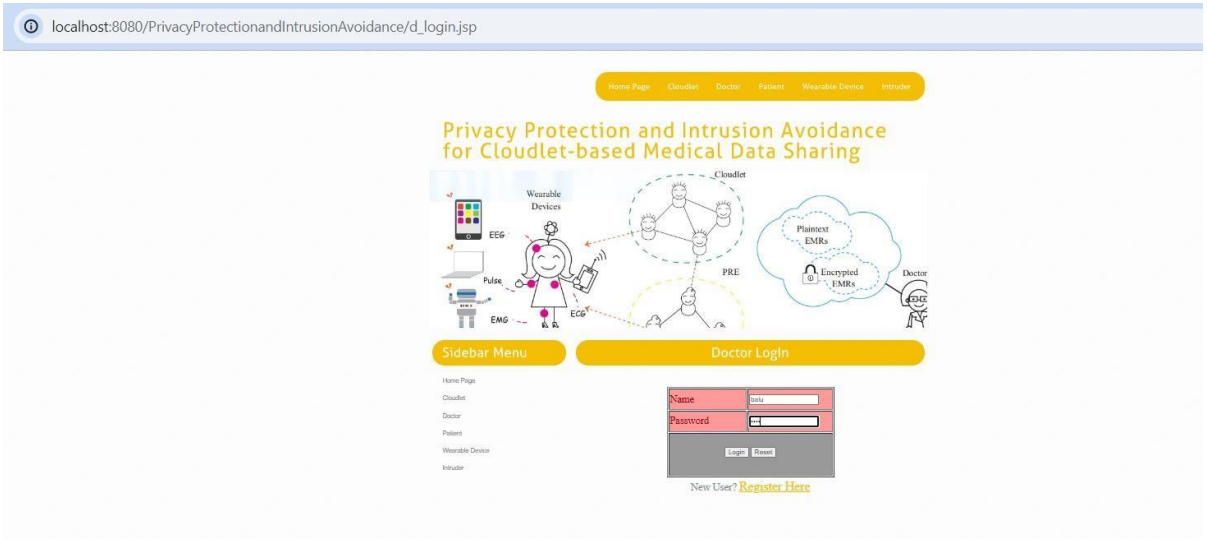


Invalid details because the login credentials are entered wrong



Login credentials are entered correctly and login page has been entered

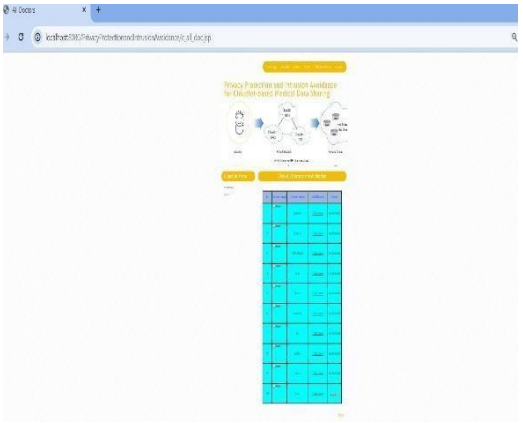
Test Case-3:



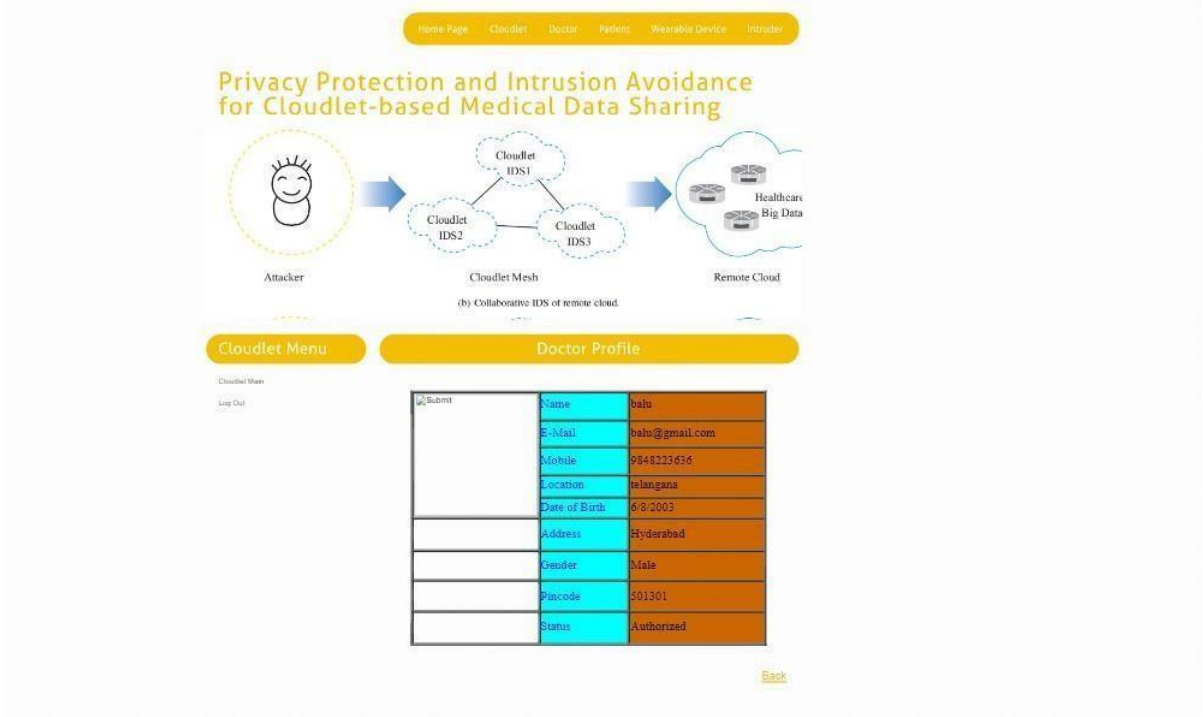
Doctor details has been given and registered successfully

You are not Authorized, Please wait!!!

Back



The doctor details has been registered successfully and waiting for authorization fromcloudet.

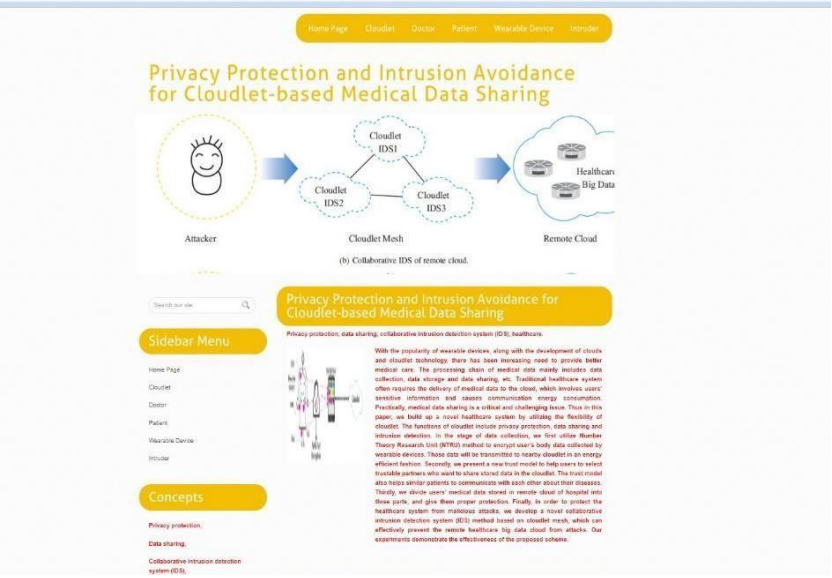


Doctor details has been successfully authorized by cloudlet.

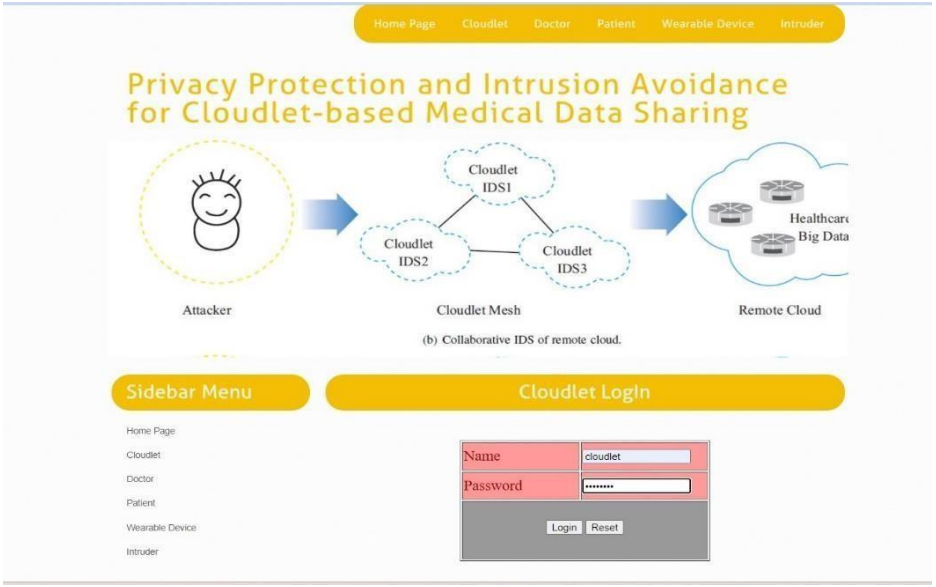
CHAPTER-8

RESULTS

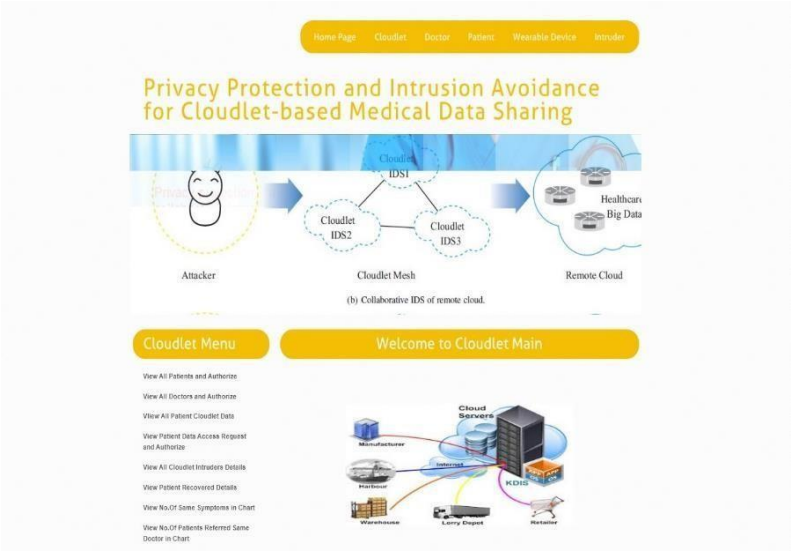
8 RESULTS



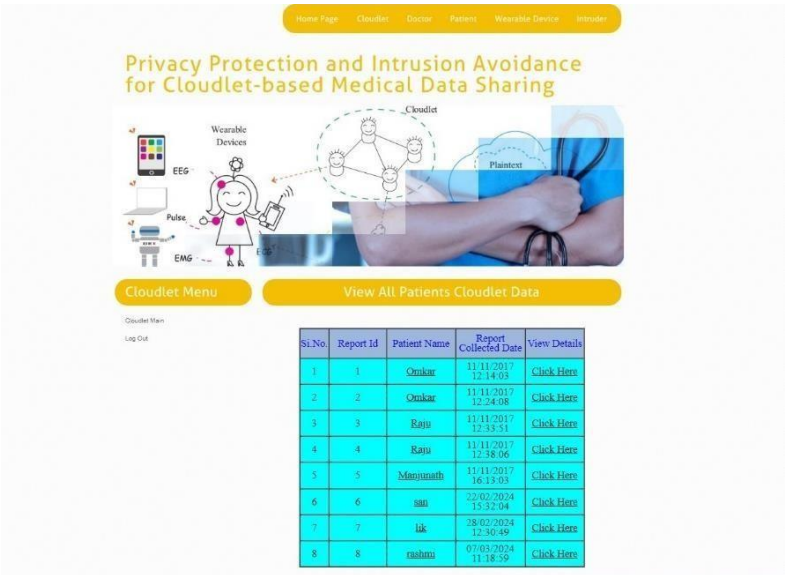
Output-1



Output-2

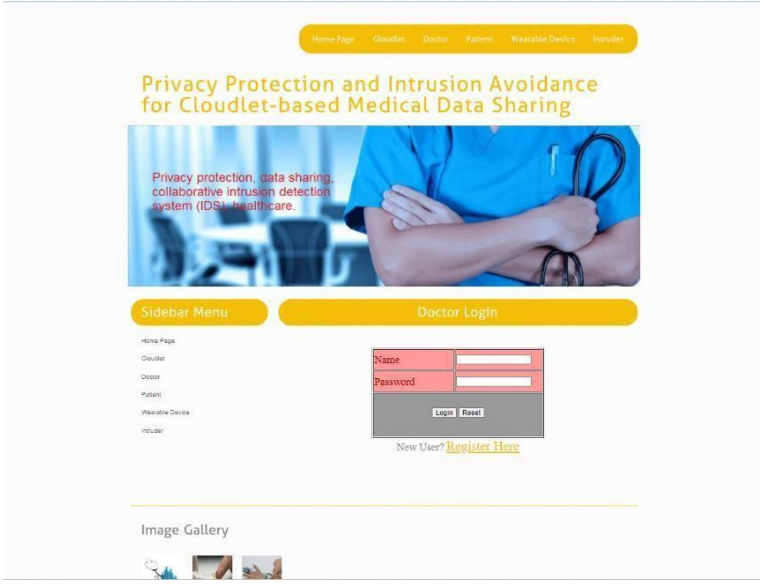


Output-3

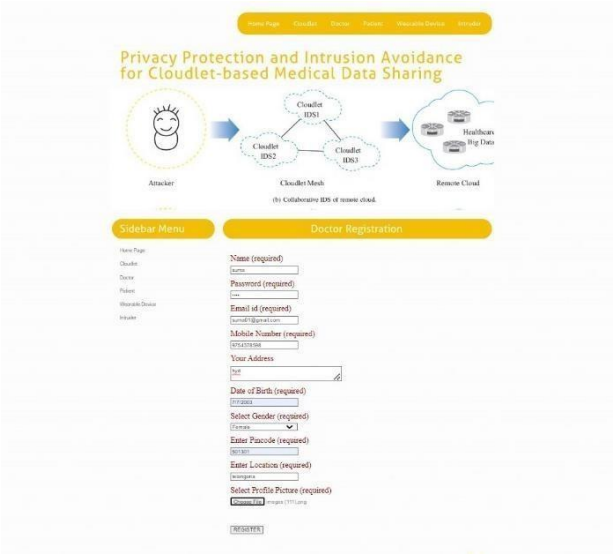


Si.No.	Report Id	Patient Name	Report Collected Date	View Details
1	1	Omkar	11/11/2017 12:14:03	Click Here
2	2	Omkar	11/11/2017 12:24:08	Click Here
3	3	Raju	11/11/2017 12:33:51	Click Here
4	4	Raju	11/11/2017 12:38:06	Click Here
5	5	Manjunath	11/11/2017 16:13:03	Click Here
6	6	san	22/02/2024 15:32:04	Click Here
7	7	ijk	28/02/2024 12:30:49	Click Here
8	8	rashmi	07/03/2024 11:18:59	Click Here

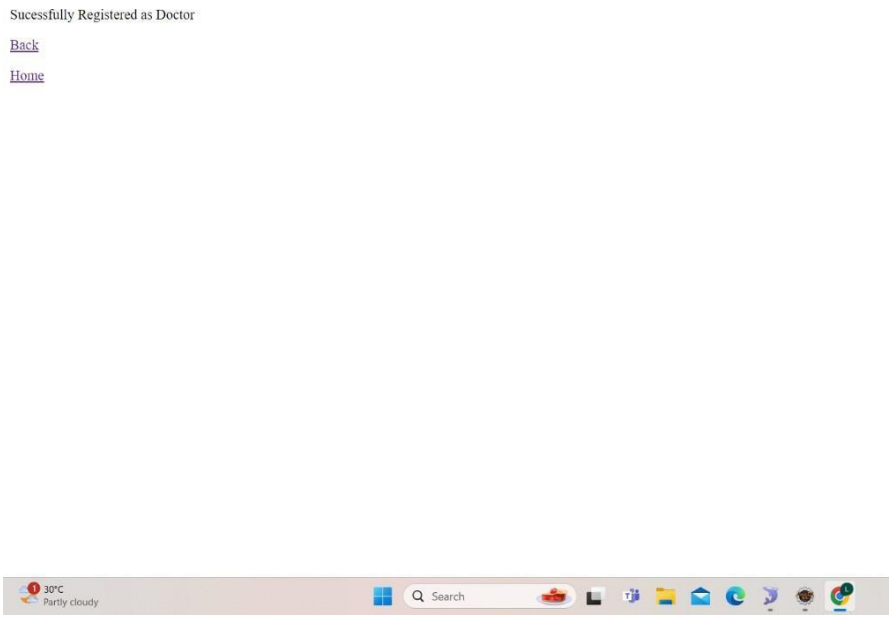
Output-4



Output-5

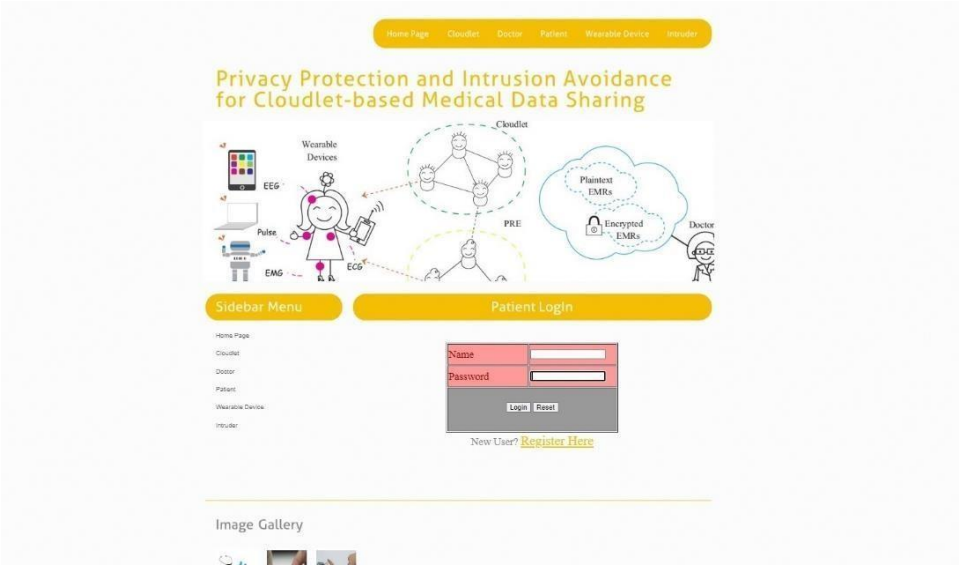


Output-6

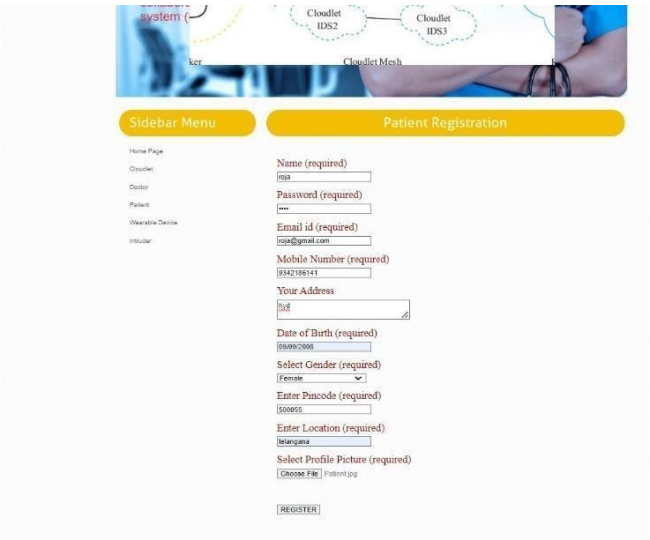


Output-7

Output-8



Output-9



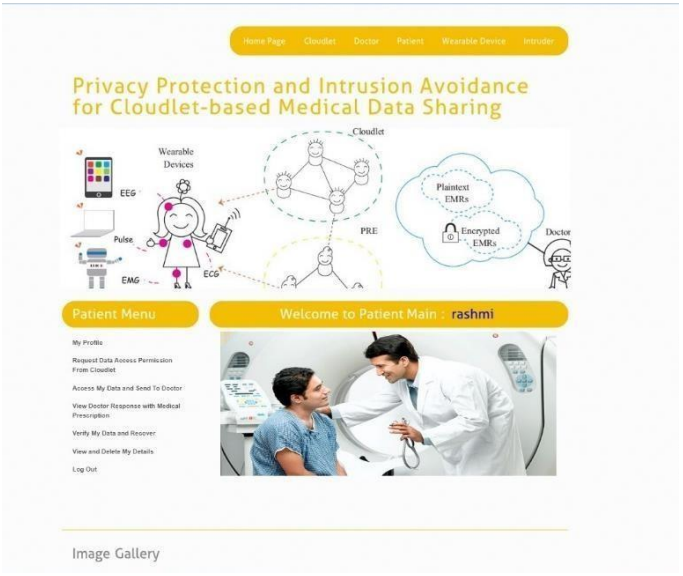
Output-10

Sucessfully Registered as Patient

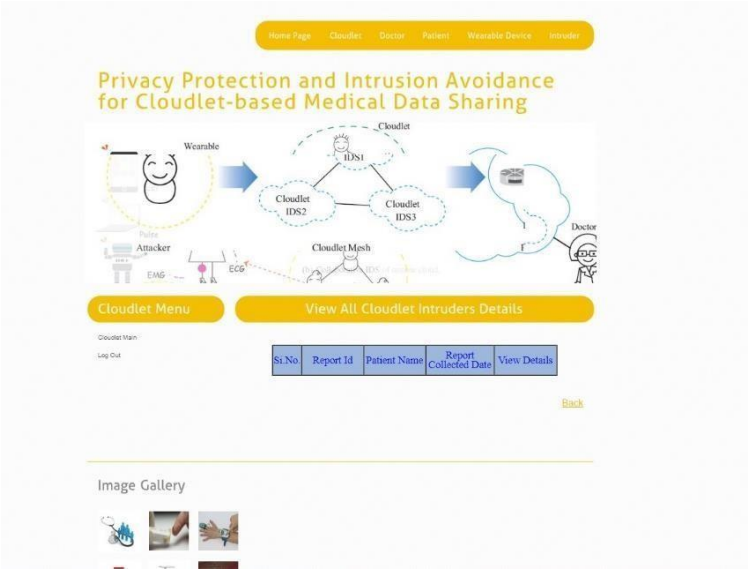
Back

Home

Output-11

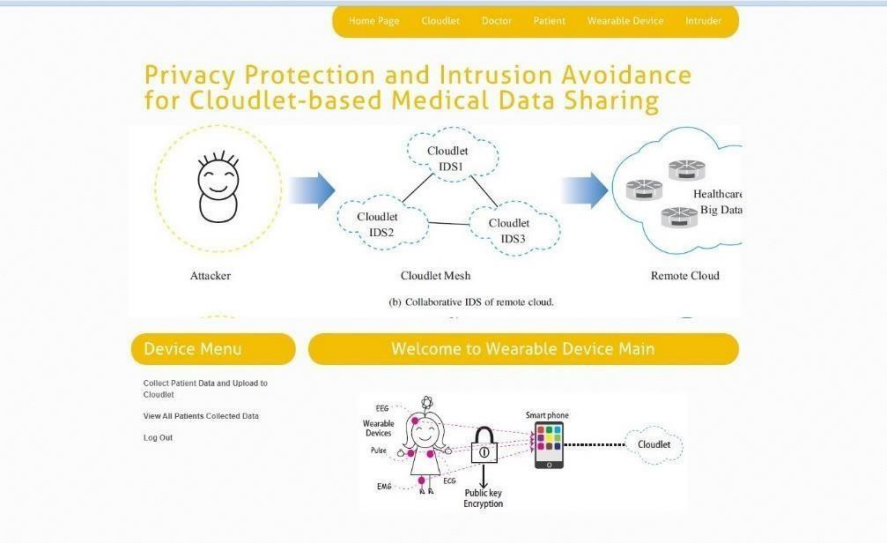


Output-12

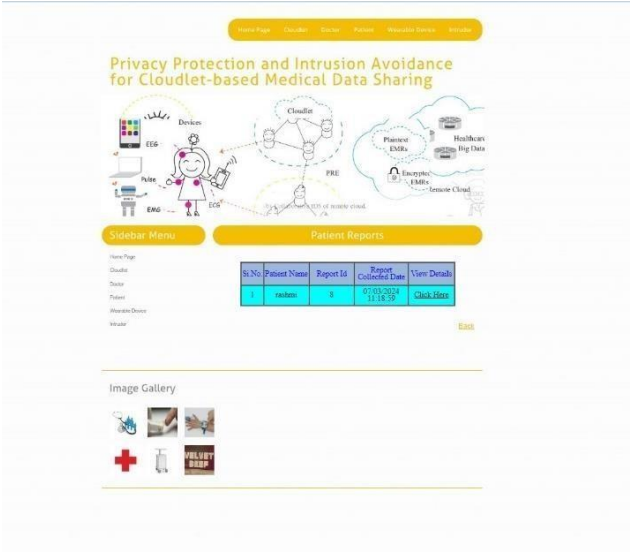


Output-13

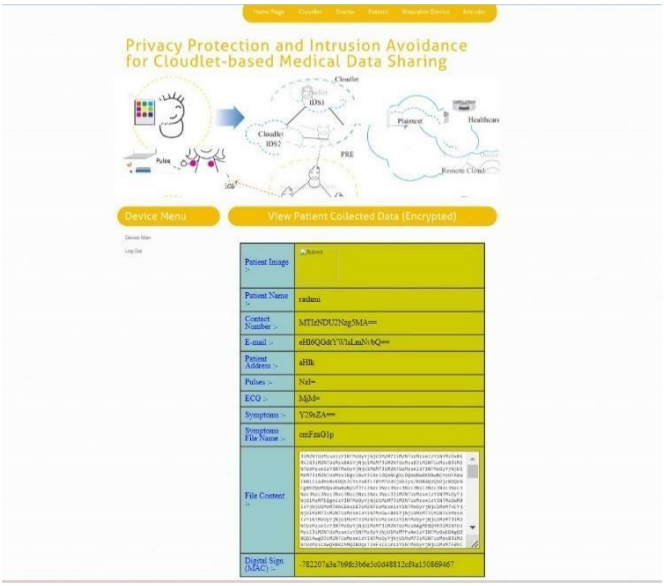
Output-14



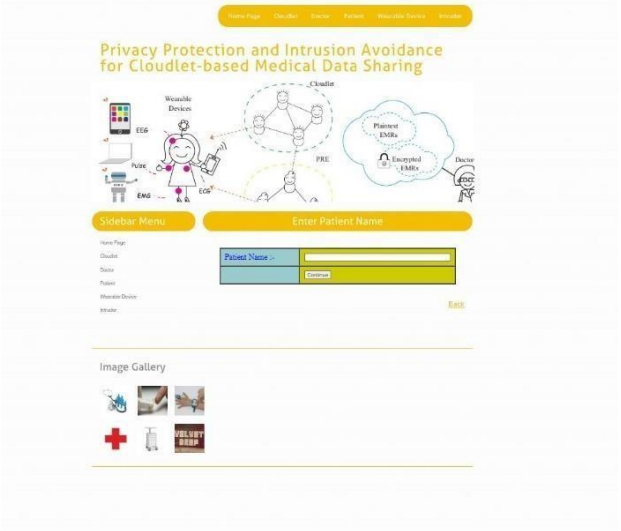
Output-15



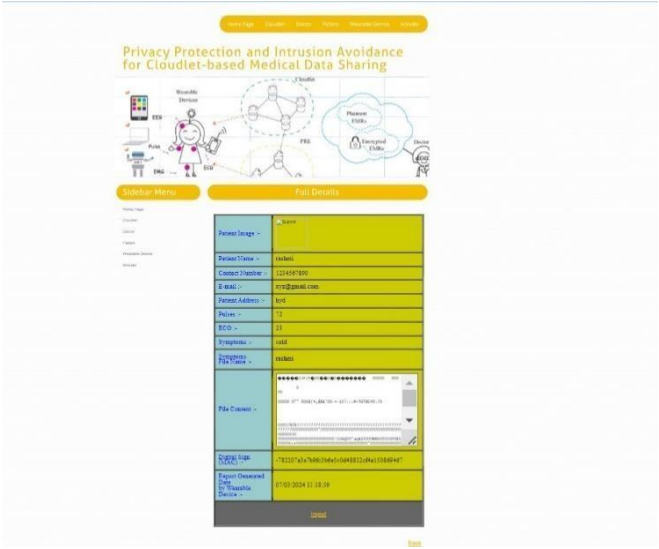
Output-16



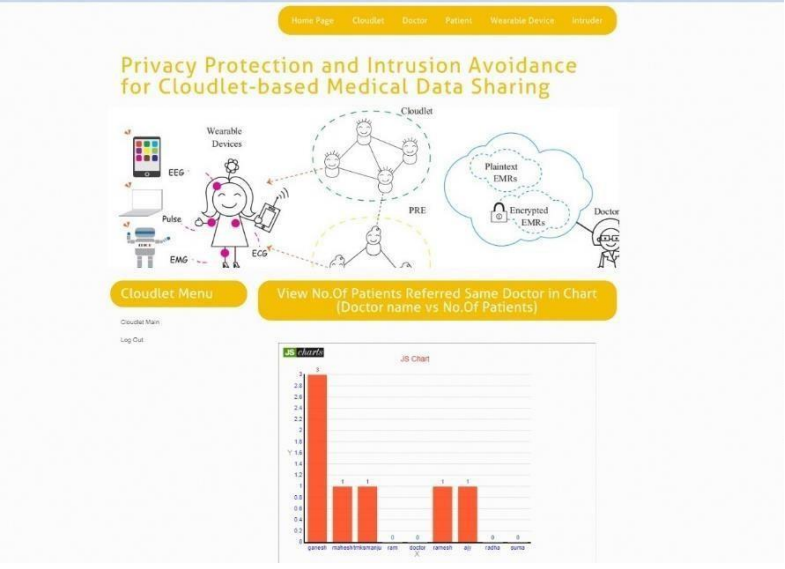
Output-17



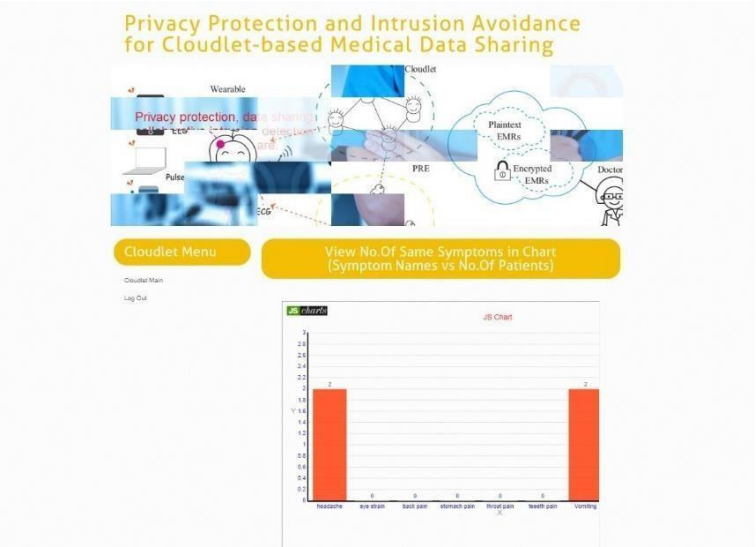
Output-18



Output-19



Output-20


Privacy Protection and Intrusion Avoidance
for Cloudlet-based Medical Data Sharing
Wearable
Cloudlet
Plaintext
EMRs
PRE
Encrypted
EMRs
Doctor
Pulse
ECG
Cloudlet Menu
View No.Of Same Symptoms in Chart
(Symptom Names vs No.Of Patients)
Cloudlet Main
Log Out
JS Chart
headache
eye strain
back pain
stomach pain
throat pain
teeth pain
Vomiting

Output-21

CHAPTER-9

CONCLUSION & FUTURE ENHANCEMENT

9 CONCLUSION & FUTURE ENHANCEMENT

Conclusion:

In this paper, we investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as wellas low communication cost. However, it does allow users to transmit data to a cloudlet, whichtriggers the data sharing problem in the cloudlet.

Firstly, we can utilize wearable devices to collect users' data, and in order to protect users privacy, we use NTRU mechanism to make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preservingof remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. The proposed schemes are validated with simulations and experiments.

Future Enhancement:

However, by making use of a hybrid cryptographic scheme of NTRU the researcher failed to

Provide peer-to-peer SMS solution in non-server architecture mobile security systems. This scheme was mainly introduced in this research to send an SMS by a doctor to patient regardingthe medical prescriptions in emergency cases. Yet, due to lack of time period, the researcher failed to attain this result. So, this scheme can be referred for the future work and the researchercan offer essential security services like confidentiality, authentication, non-repudiation and integrity.

Cloudlets and remote clouds to protect and share critical healthcare data. We created a mechanism to stop users from transferring information to distant clouds, guaranteeing that collected data is secure and reducing connection costs. Data sharing issues could arise for users migrating data to Cloudlet. To protect user privacy, we use the NTRU approach to securely encrypt the data transmission to Cloudlets. Based on the user's level of trust, we apply a trust model to decide whether to publish data in Cloudlet. It also distributes and encrypts remote cloud data in a number of ways while boosting transmission efficiency in order to safeguard data privacy. The next item on the agenda is a Cloudlet mesh-based joint IDS to protect the entire network.

CHAPTER 10
BIBLIOGRAPHY

10 BIBLIOGRAPHY

[1] K. Hung, Y. Zhang, and B. Tai, “Wearable medical devices for tele home healthcare,” in Engineering in Medicine and Biology Society, 2004. IEMBS’04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, “Cloud-supported cyber–physical localization framework for patients monitoring,” 2015.

[3] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, “A security framework in g-hadoop for big data computing across distributed cloud data centres,” Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[4] M. S. Hossain and G. Muhammad, “Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring,” Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, “Deypos: Deduplicatable dynamic proof of storage for multi-user environments,” 2016.

[7] L. Griffin and E. De Leastar, “Social networking healthcare,” in Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, “Big video data for light-field-based 3d telemedicine,” IEEE Network, vol. 30, no. 3, pp. 30–38, 2016.

[9] “https://www.patientslikeme.com/.”

[10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and security for online social networks: challenges and opportunities,” Network, IEEE, vol. 24,no. 4, pp. 13–18, 2010.