PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING

A dissertation submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF COMPUTER APPLICATIONS

of

University of Mysore

By

PRAVEEN N	**BC201172**
RAHUL S	**BC201181**
ROHITH KUMAR S	**BC201189**
SHEREYAS M V	**BC201204**

Under the Guidance of:

PRAPULLA GOWDA M P

Assistant Professor, Dept of BCA

Mysuru

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS
BGS FIRST GRADE COLLEGE
MYSURU-23

2021-2022

DECLARATION

We, student of final semester BCA of BGS First Grade College, Mysuru, hereby declare that the dissertation entitled "**PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**" has been independently carried at "**BGS First Grade College**", Mysuru and submitted in partial fulfillment of the requirement for the award of **Bachelor of Computer Applications** affiliated to the **University of Mysore**, during the academicyear 2022 – 2023. Further the matter embodied in the report is an original and bonafide work doneby us.

To our knowledge this dissertation has not been submitted to any other college or universityor published at any time prior to this.

Place: Mysuru

Date:

PRAVEEN N	**BC201172**
RAHUL S	**BC201181**
ROHITH KUMAR S	**BC201189**
SHEREYAS M V	**BC201204**

BGS FIRST GRADE COLLEGE

MYSURU-23

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

CERTIFICATE

This is to Certify that "**PRAVEEN.N**" bearing "**BC201172**" has completed his/her final semester project work entitled "**PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**" as a partial fulfillment for the award of Bachelor of ComputerApplications of University of Mysore during the year 2022-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirement in respect of project workprescribed for the said degree.

Internal Guide:

PRAPULLA GOWDA M P

Asst. Professor, Dept of
BCA,BGS FGC, Mysuru.

Mr. Hareesha.C
Assistant Professor & HOD
Dept of BCA, BGS FGC, Mysuru.

Dr. R.S. Narasegowda
Principal,
BGS FGC,Mysuru.

Examiner's Name & Signature

1. **2.**

BGS FIRST GRADE COLLEGE

MYSURU-23

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

CERTIFICATE

This is to Certify that "**RAHUL.S**" bearing "**BC201181**" has completed his/her final semester project work entitled "**PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**" as a partial fulfillment for the award of Bachelor of ComputerApplications of University of Mysore during the year 2022-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirement in respect of project workprescribed for the said degree.

Internal Guide:

PRAPULLA GOWDA M P

Asst. Professor, Dept of
BCA,BGS FGC, Mysuru.

Mr. Hareesha.C
Assistant Professor & HOD
Dept of BCA, BGS FGC, Mysuru.

Dr. R.S. Narasegowda
Principal,
BGS FGC,Mysuru.

Examiner's Name & Signature

1. **2.**

BGS FIRST GRADE COLLEGE

MYSURU-23

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

CERTIFICATE

This is to Certify that "**ROHITH KUMAR.S**" bearing "**BC201189**" has completed his/her final semester project work entitled "**PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**" as a partial fulfillment for the award of Bachelor of ComputerApplications of University of Mysore during the year 2022-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirement in respect of project workprescribed for the said degree.

Internal Guide:

PRAPULLA GOWDA M P

Asst. Professor, Dept of
BCA,BGS FGC, Mysuru.

Mr. Hareesha.C
Assistant Professor & HOD
Dept of BCA, BGS FGC, Mysuru.

Dr. R.S. Narasegowda
Principal,
BGS FGC,Mysuru.

Examiner's Name & Signature

1. **2.**

BGS FIRST GRADE COLLEGE

MYSURU-23

DEPARTMENT OF BACHELOR OF COMPUTER APPLICATIONS

CERTIFICATE

This is to Certify that "**SHEREYAS.M V**" bearing "**BC201204**" has completed his/her final semester project work entitled "**PRIVACY PROTECTION AND INTRUSION AVOIDENCE FOR CLOUDLET-BASED MEDICAL DATA SHARING**" as a partial fulfillment for the award of Bachelor of ComputerApplications of University of Mysore during the year 2022-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report. The project report has been approved as it satisfies the academic requirement in respect of project workprescribed for the said degree.

Internal Guide:

PRAPULLA GOWDA M P

Asst. Professor, Dept of
BCA,BGS FGC, Mysuru.

Mr. Hareesha.C
Assistant Professor & HOD
Dept of BCA, BGS FGC, Mysuru.

Dr. R.S. Narasegowda
Principal,
BGS FGC,Mysuru.

Examiner's Name & Signature

1. **2.**

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 project, 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 proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks.

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragementcrowned our efforts with success.

We consider it as a privilege to express our sincere gratitude and respect to all those who guidedme during the completion of the project.

We would like to extend our sincere **thanks Dr.R.S.Narasegowda, Principal, BGS FGC, Kuvempunagar, Mysuru** for providing the facilities to complete this project.

We express our deep-felt sincere gratitude to **Mr.Hareesha.C, HOD Department of BCA,** forhis encouragement and immense help.

We thank our internal guide "**Prapulla Gowda M P**", Assistant Professor, Dept. of BCA, for his/her inspiration, encouragement, timely guidance and valid suggestion throughout our project.

Finally, we wish to thank all the staff members and non-teaching staff of our department for their help and guidance.

Above all, my sincere gratitude to our parents and friends, also those who have directly or indirectly helped me to complete this project successfully.

PRAVEEN N	**BC201172**
RAHUL S	**BC201181**
ROHITH KUMAR S	**BC201189**
SHEREYAS M V	**BC201204**

TABLE OF CONTENT

CHAPTER 1

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' evergrowing 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 to facilitate the trace of the disease treatment process for the retrieval of real-time disease information. Healthcare social platform, such as PatientsLike 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 entails 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 data are 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 of cloudlet. 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 users to 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 collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

1:1 Objective of the Project:

- The main objective of this project is to investigate the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud.
- There is a need to develop a system, which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost.
- Another main objective of this project is to give privacy-preserving remote cloud data.

CHAPTER 2

Literature Survey

2:1 LITERATURE REVIEW

2:1:1 Title: Data Security and Vulnerability Prevention for Cloudlet-Based Medical Data Sharing

Authors: M. Purushotham Reddy; A. Md. Faisal Anwar; A. Sahithi; A. K. Shravani

In this paper, another arrangement of medical services is built by utilizing cloud adaptability. The cloudlet capacities incorporate security of protection, information sharing, and interruption discovery. During data collection, a method for encrypting data from user corpses collected through wearable devices by the Number Theory Research Unit (NTRU) is used. These data are energy-efficiently transmitted to the nearby cloud. Second, a new model of confidence which helps users to select reliable cloud data partners is introduced. The trust model additionally assists patients with imparting their infections. Third, appropriate protection of the medical data of users stored in the hospital remote cloud are divided into three parts. A new collaborative intrusion detection method (IDS) is developed to protect the prosperity system against malice attacks, in light of the lattice for cloud, which can successfully stay away from assaults by the distant medical care huge information cloud.

2:1:2 Title: Cyber security and Data Privacy in the Cloudlet for Preliminary Healthcare Big Data Analytics

Authors: Tariq Javid; Muhammad Faris; Hira Beenish; Muhammad Fahad

In cyber physical systems, cybersecurity and data privacy are among most critical considerations when dealing with communications, processing, and storage of data. Geospatial data and medical data are examples of big data that require seamless integration with computational algorithms as outlined in Industry 4.0 towards adoption of fourth industrial revolution. Healthcare Industry 4.0 is an application of the design principles of Industry 4.0 to the medical domain. Mobile applications are now widely used to accomplish important business functions in almost all industries. These mobile devices,

however, are resource poor and proved insufficient for many important medical applications. Resource rich cloud services are used to augment poor mobile device resources for data and compute intensive applications in the mobile cloud computing paradigm. However, the performance of cloud services is undesirable for data-intensive, latency-sensitive mobile applications due increased hop count between the mobile device and the cloud server. Cloudlets are virtual machines hosted in server placed nearby the mobile device and offer an attractive alternative to the mobile cloud computing in the form of mobile edge computing. This paper outlines cybersecurity and data privacy aspects for communications of measured patient data from wearable wireless biosensors to nearby cloudlet host server in order to facilitate the cloudlet based preliminary and essential complex analytics for the medical big data

2:1:3 Title: The Effective Dashboard to Control the Intrusion in the Private Protection of the Cloudlet Based on the Medical Mutual Data Using ECC

Authors: AB Navya; B M Chandrakala

Taking the consideration of the popularity of the adoptable devices with respect to the cloud development methodologies and strategies, its mandatory need to take better caution of the medical data care. The hierarchical chain of the data(medical) is mainly considers collection various attributed data, solid storage of data and mutual sharing across the clouds. As regular approaches of health care methodologies the entire dashboard or ongoing system needs regularly to broadcast with energy consumption. Practially mutual sharing of the data is quite huge challenging issue. So this work is developed a novel and hierarchical dashboard by using the ease of the cloud let system. the methods of the relevant cloud adds the private functionality for protection and mutual data sharing for intrusion discovery. One particular stage of entire process of data gathering our work first takes Number theory discovery model snippet to do encryption the user's wearable devises on body. So that data will be broadcasted to closest cloud with feasible and efficient energy fashion. Next flow this work continues a new trust worthy method to give the feasibility for users to choose the neighbours who needs the mutual share of the data in the cloud. The trust worthy model serves same patients to broadcast each other about the effected deceases. Next on going process the dashboard divides the data in third party cloud of hospital hooked on various portions then provides them decent fortification by using elliptic curve cryptography (ecc).

2:2 Problem Statement

Medical data sharing is a critical and challenging issue. Thus in this project, 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. Also there is a need to protect the whole system from malicious attacks.

CHAPTER 3

SYSTEM ANALYSIS

3:1 EXISTING SYSTEM

- ✓ Lu et al. proposed a system called SPOC, which stands for the secure and privacy-preserving opportunistic computing framework, was proposed to treat the storage problem of healthcare data in a cloud environment and addressed the problem of security and privacy protection under such an environment.
- ✓ Cao et al., an MRSE (multikeyword 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. Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome.
- ✓ In Zhang et al., a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare data in cloud assisted wireless body area network (WBANs).

3:1:1 Disadvantages

- Causes communication energy consumption.
- Practically, medical data sharing is a critical and challenging issue
- No Trust.

3:2 PROPOSED SYSTEM

- This project proposes a cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are 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 of cloudlet. 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 users to 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 collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

3:2:1 Advantages

- 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 trust model. 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 system against malicious attacks.

3:3 Functional Requirement:

1. **Cloudlet**
2. **Wearable Device**
3. **Doctor**
4. **Patient**

1. **Cloudlet**
    - Login
    - View Patients and Authorize
    - View Doctors and Authorize
    - View all patients data
    - View the Access request and give permission
    - View the attackers
    - Logout

2. **Wearable Device**
    - Login
    - Collect the patient data and upload it to cloudlet
    - View all patients collected data
    - Logout

3. **Doctor**
    - Register
    - Login
    - View the patient details and he can suggest medicines.
    - View all suggested medicine for the patient
    - Logout

4. **Patient**
    - Register
    - Login
    - Send a request to cloudlet to access the medical details
    - Access the data and send it to the doctor
    - View the doctor resonance with medical prescription
    - Verify the medical file
    - View all medical files and delete it
    - Logout

3:4 Non-Functional Requirements:

3:4:1 Maintainability

Maintainability is the ease with which a product can be maintained in order to:

- Correct defects or their cause,
- Repair or replace faulty or worn-out components without having to replace still working parts,
- Prevent unexpected working condition,
- Maximize a product's useful life,
- Maximize efficiency,
- Reliability and safety,
- Meet new requirements,
- Make future maintenance easier, or
- Cope with a changed environment.

3:4:2 Portability

Software portability may involve

- Transferring installed program files to another computer of basically the same architecture.
- Reinstalling a program from distribution files on another computer of basically the same architecture.
- Building executable programs for different platforms from source code; this is what is usually understood by "porting".

3:4:3 Usability

The primary notion of usability is that an object designed with a generalized users' psychology and physiology in mind is, for example:

- More efficient to use—takes less time to accomplish a particular task
- Easier to learn—operation can be learned by observing the object
- More satisfying to use

3:4:4 Reliability

The objectives of reliability engineering, in decreasing order of priority, are

- To apply engineering knowledge and specialist techniques to prevent or to reduce the likelihood or frequency of failures.
- To identify and correct the causes of failures that do occur despite the efforts to prevent them.
- To determine ways of coping with failures that do occur, if their causes have not been corrected.
- To apply methods for estimating the likely reliability of new designs, and for analysing reliability data.

3:4:5 Consistent uptime

The new system will be able to stay up and running at least 98% of the time. Any downtime would be due to maintenance or upgrades. This downtime also includes any potential failures/crashes.

3:4:6 Load and concurrency

The system must be able to serve at least two thousand users concurrently without crashing.

3:4:7 Dealing with large quantities of data

The developed system will have to deal with large quantities of data and a large number of users accessing the data at once. The large quantity of data includes timetable information and data retrieved from the database by many users at the same time.

3:4:8 Familiar Interface

The new system will have an interface that shares some of the feel of the old system so that users who are familiar with the old system will not have trouble adjusting to the new system.

3:4:9 Real-time Feedback

The new registration system should display the student's timetable and show the changes made to it in real-time as the student adds and drops courses.

3:4:10 Focused Layout

The new system will reduce the potential for confusion by having a focused layout. This means that it will display information that is relevant to the current task and conversely, leave out irrelevant information.

3:4:11 Web Accessibility

The new system will be compatible with screen readers to assist the visually impaired. This means that screen readers should interpret the displayed text into speech and should not output anything that does not correspond to displayed text. It is also important that the colours are designed so that colour-blind people can still distinguish changes in content.

3:4:12 Effective Recovery

The system must effectively recover from a crash within ten minutes. Effective recovery means that the data is still in a consistent state accurate to 1 minute before the system crashes when the system returns.

3:5 SYSTEM REQUIREMENTS:

3:5:1 HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

3:5:2 SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Tomcat server, Java JDK, Notepad ++
- Database : MYSQL

3:6 Feasibility Study

- **What is Feasibility Study?**

Feasibility study is the process of determination of whether or not a project is worth doing. Feasibility studies are undertaken within tight time constraints and normally culminate in a written and oral feasibility report. The contents and recommendations of this feasibility study helped us as a sound basis for deciding how to precede the project. It helped in taking decisions such as which software to use, hardware combinations, etc. The following is the process diagram for feasibility analysis. In the diagram, the feasibility analysis starts with the user set of requirements. With this, the existing system is also observed. The next step is to check for the deficiencies in the existing system. By evaluating the above points a fresh idea is conceived to define and quantify the required goals. The user consent is very important for the new plan.

Along with, for implementing the new system, the ability of the organization is also checked. Besides that, a set of alternatives and their feasibility is also considered in case of any failure in the proposed System. Thus, feasibility study is an important part in software development.

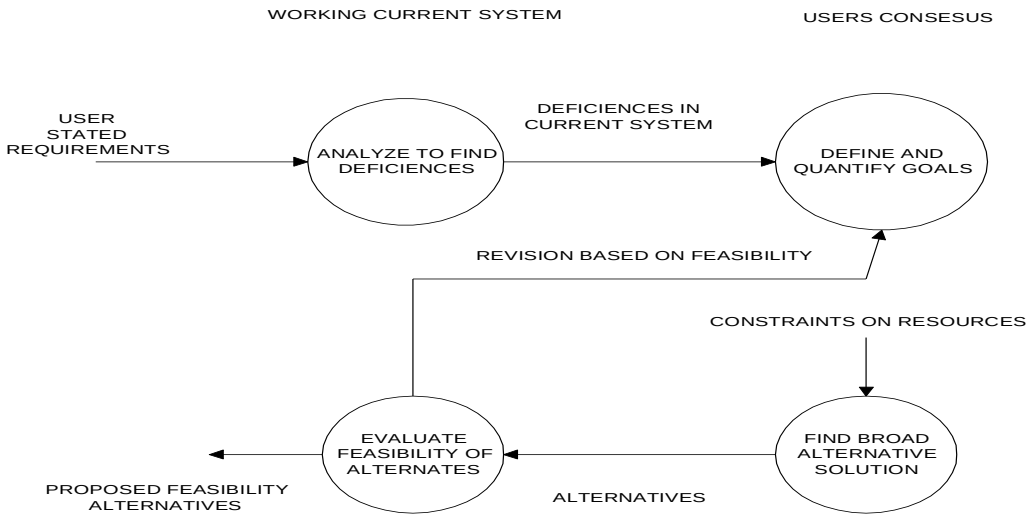


Figure: PROCESS DIAGRAM FOR FEASIBILITY ANALYSIS

3:6:1 Technical Feasibility:

Technical feasibility determines whether the work for the project can be done with the existing equipment, software technology and available personnel. Technical feasibility is concerned with specifying equipment and software that will satisfy the user requirement.

This project is feasible on technical remarks also, as the proposed system is more beneficiary in terms of having a sound proof system with new technical components installed on the system. The proposed system can run on any machines supporting Windows and Internet services and works on the best software and hardware that had been used while designing the system so it would be feasible in all technical terms of feasibility.

Technical Feasibility Addresses Three Major Issues:

1. Is the proposed Technology or Solution Practical?

The technologies used are matured enough so that they can be applied to our problems. The practicality of the solution we have developed is proved with the use of the technologies we have chosen. The technologies such as JAVA (JSP, Servlet), JavaScript and the compatible H/Ws are so familiar with the today's knowledge based industry that anyone can easily be compatible to the proposed environment.

2. Do we currently possess the necessary technology?

We first make sure that whether the required technologies are available to us or nor. If they are available then we must ask if we have the capacity. For instance, “Will our current Printer be able to handle the new reports and forms required of a new system?

3. Do we possess the necessary Technical Expertise and is the Schedule reasonable?

This consideration of technical feasibility is often forgotten during feasibility analysis. We may have the technology, but that does not mean we have the skills required to properly apply that technology. As far as our project is concerned, we have the necessary expertise so that the proposed solution can be made feasible.

3:6:2 Economical Feasibility:

Economical feasibility determines whether there are sufficient benefits in creating to make the cost acceptable, or is the cost of the system too high. As this signifies cost, benefit analysis and savings. On the behalf of the cost-benefit analysis, the proposed system is feasible and is economical regarding its pre-assumed cost for making a system. During the economical feasibility test we maintained the balance between the Operational and Economical feasibilities,

as the two were the conflicting. For \example, the solution that provides the best operational impact for the end-users may also be the most expensive and, therefore, the least economically feasible. We classified the costs of Online Counselling according to the phase in which they occur. As we know that the system development costs are usually one-time costs that will not recur after the project has been completed. For calculating the Development costs we evaluated certain cost categories viz.

- Personnel costs
- Computer usage
- Training

In order to test whether the Proposed System is cost-effective or not we evaluated it through three techniques viz.

- Return on Investment
- Net Present value

3:6:3 Operational Feasibility:

Operational feasibility criteria measure the urgency of the problem (survey and study phases) or the acceptability of a solution (selection, acquisition and design phases). Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.

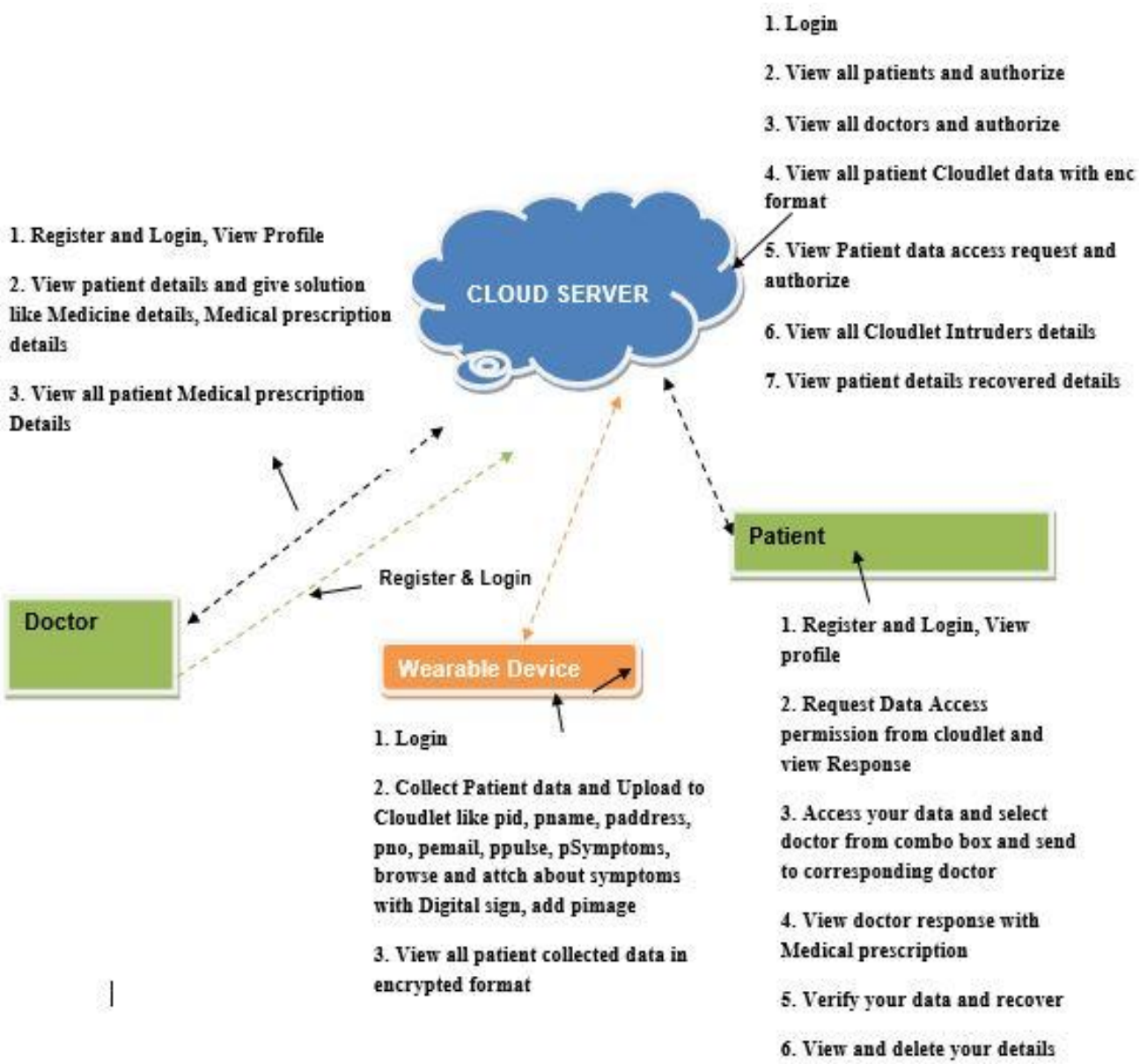
The operational feasibility assessment focuses on the degree to which the proposed development project fits in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture and existing business processes.

To ensure success, desired operational outcomes must be imparted during design and development.

CHATER 4

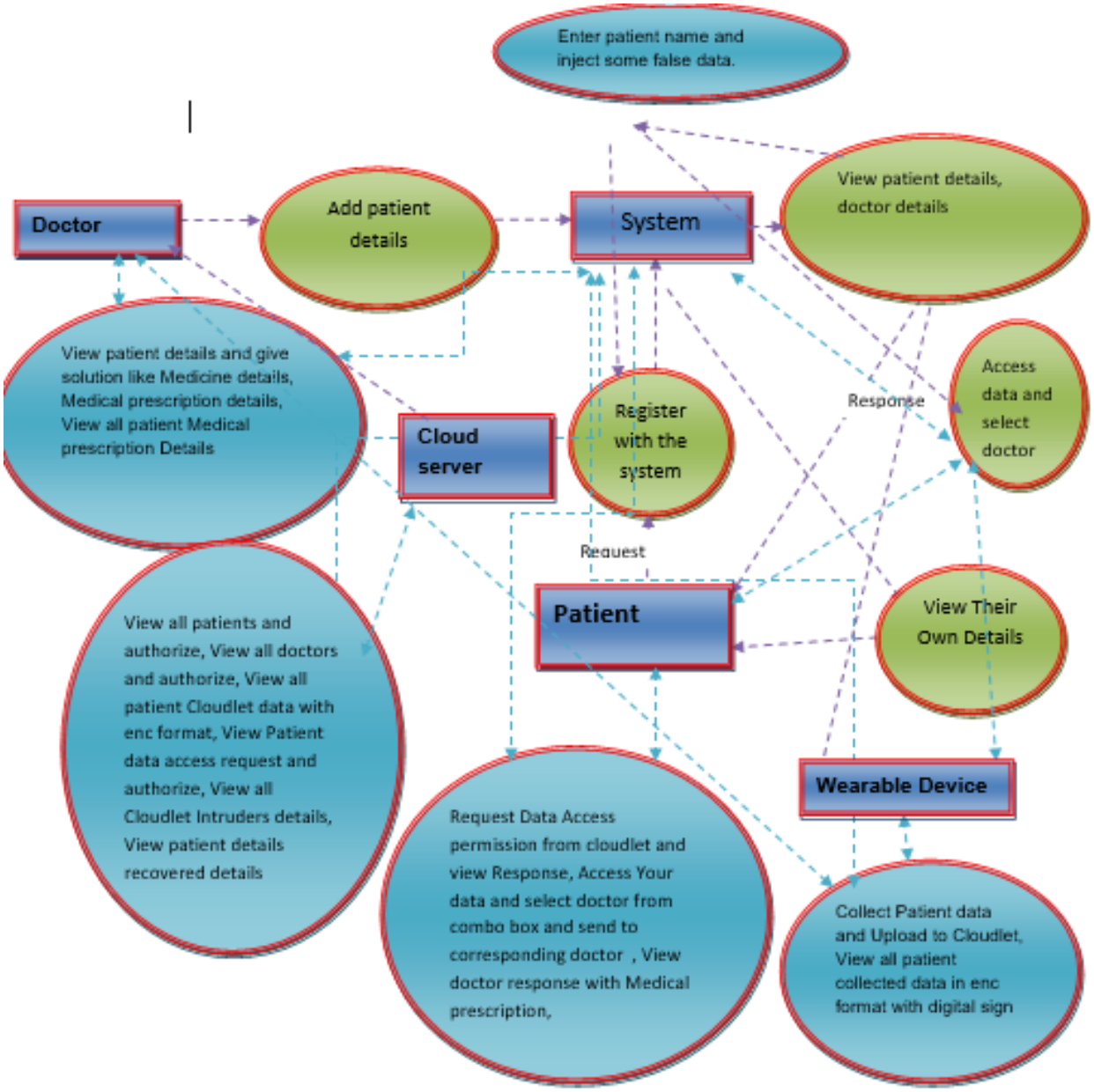
SYSTEM DESIGN

4:1 System Architecture:



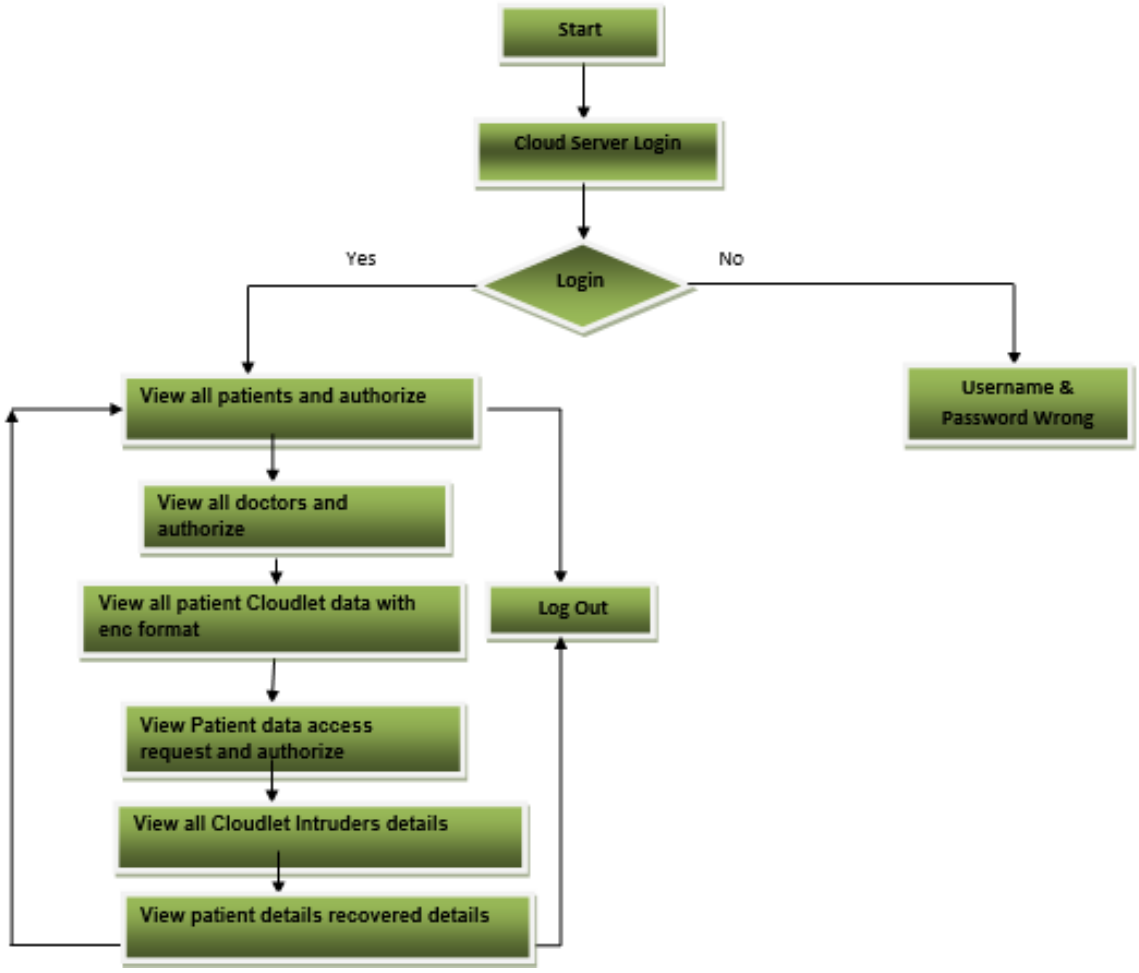
4:2 DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

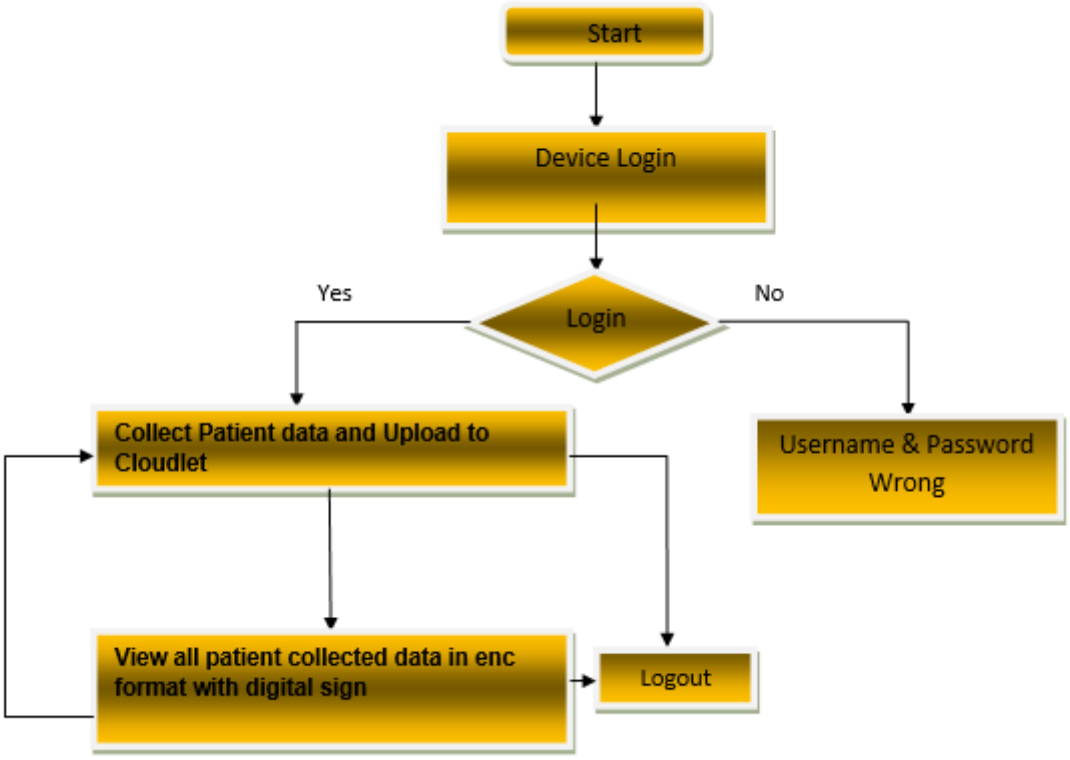

Enter patient name and inject some false data.
Doctor
Add patient details
System
View patient details, doctor details
View patient details and give solution like Medicine details, Medical prescription details, View all patient Medical prescription Details
Cloud server
Register with the system
Response
Access data and select doctor
Request
Patient
View Their Own Details
View all patients and authorize, 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, View patient details recovered details
Wearable Device
Request Data Access permission from cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor , View doctor response with Medical prescription,
Collect Patient data and Upload to Cloudlet, View all patient collected data in enc format with digital sign

4:3 FLOW CHART:

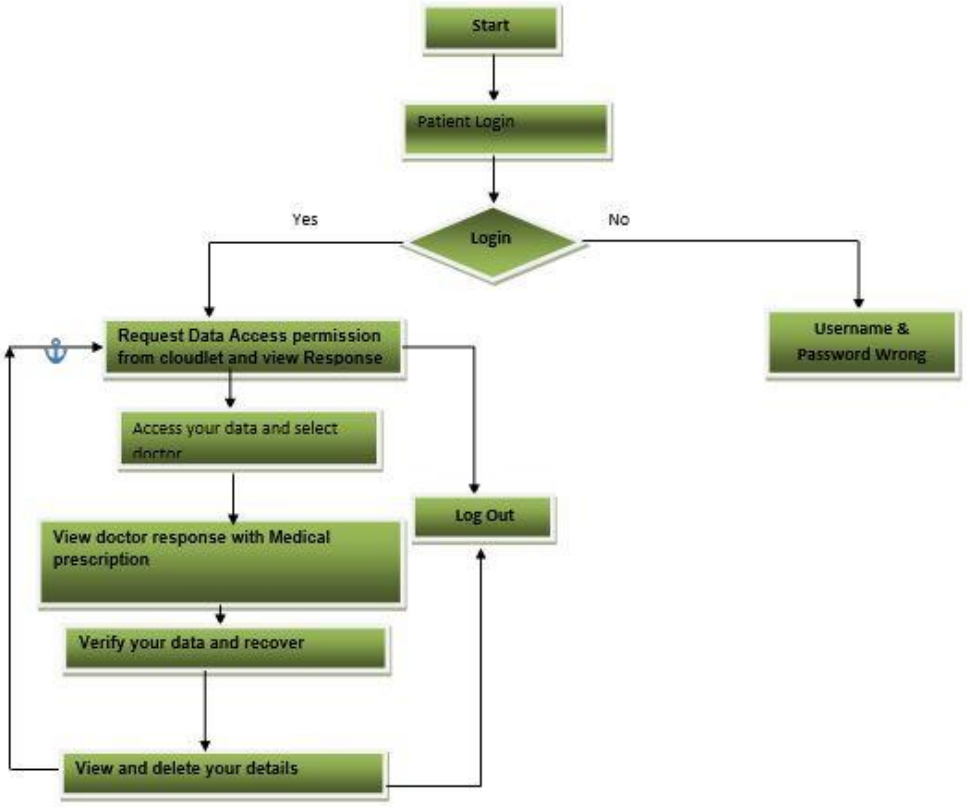
4:3:1 Flow Chart: Admin



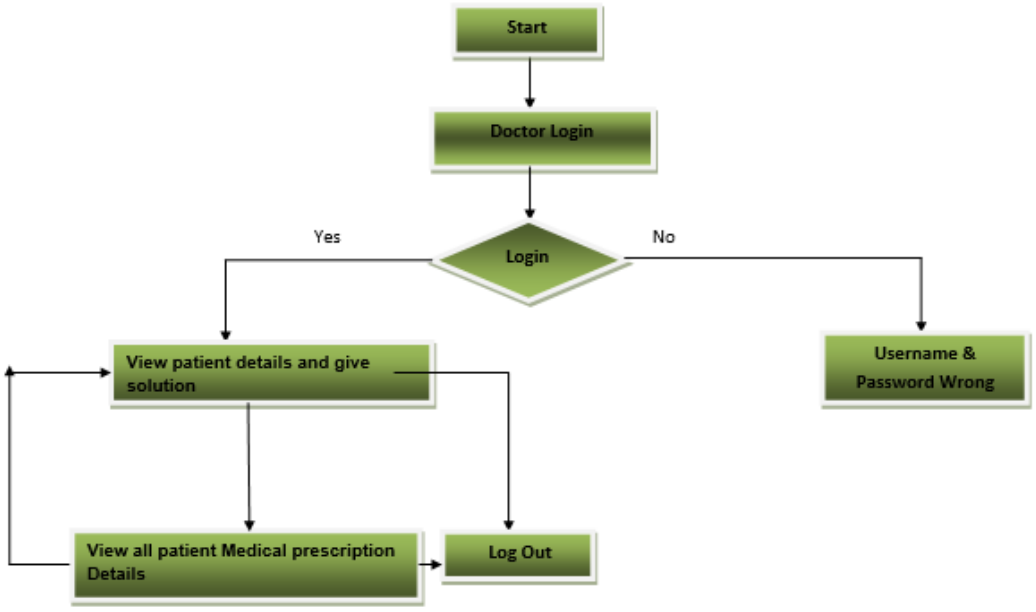
4:3:2 Flow Chart: Wearable Device



4:3:3 Flow Chart: Patient



4:3:4 Flow Chart: Doctor



4:4 UML DIAGRAMS:

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group.

The goal is for UML to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: a Meta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

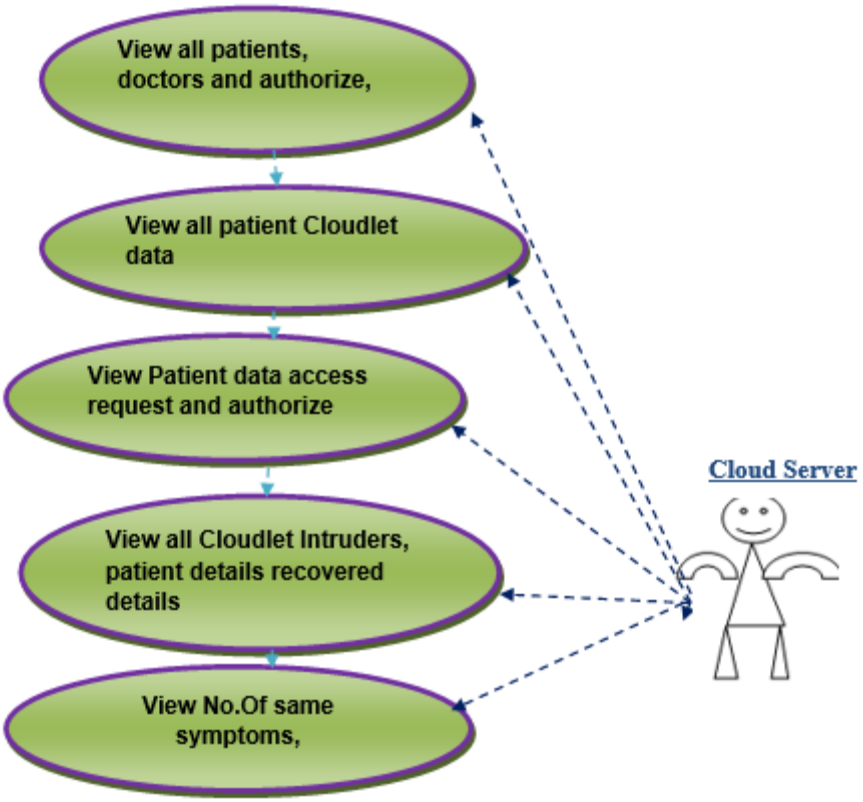
4:4:1 GOALS:

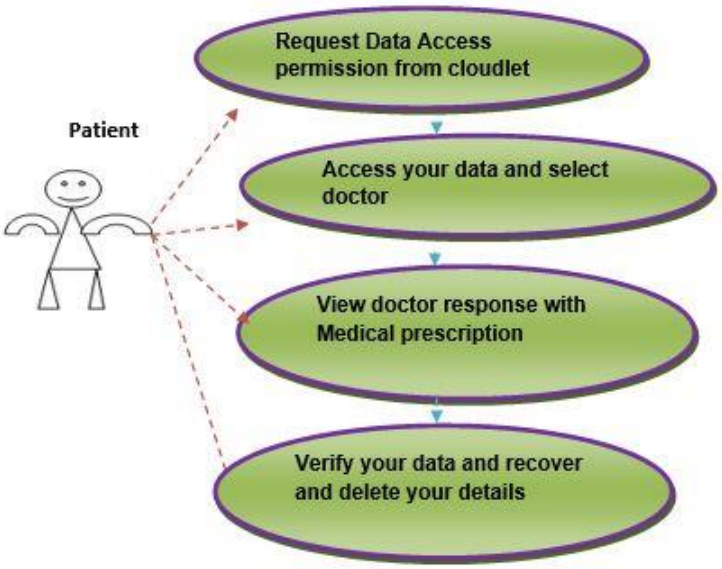
The Primary goals in the design of the UML are as follows:

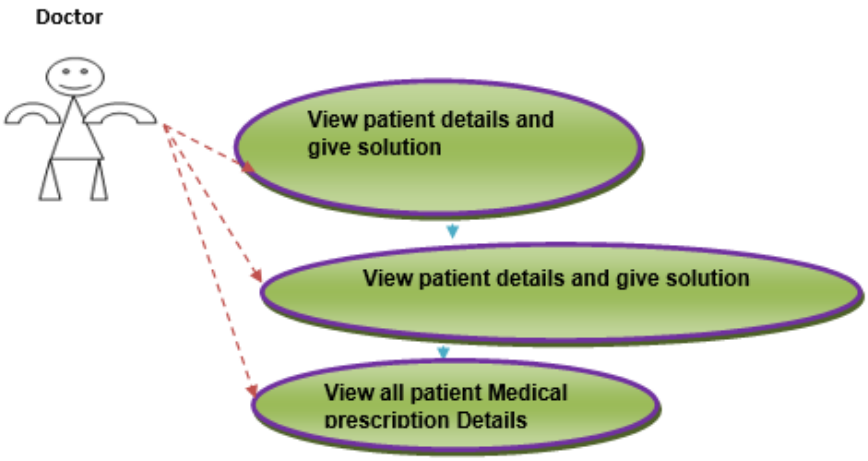
1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.
2. Provide extendibility and specialization mechanisms to extend the core concepts.
3. Be independent of particular programming languages and development process.
4. Provide a formal basis for understanding the modeling language.
5. Encourage the growth of OO tools market.
6. Support higher level development concepts such as collaborations, frameworks, patterns and components.
7. Integrate best practices

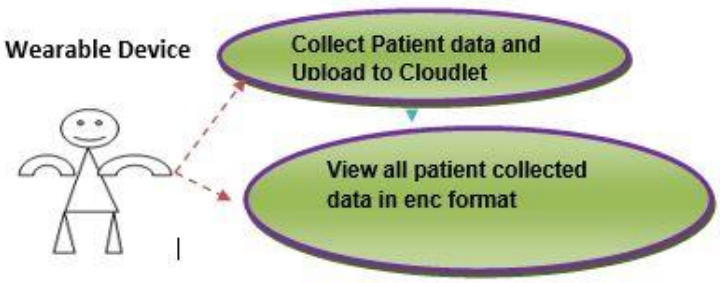
4:5 USE CASE DIAGRAM:

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.



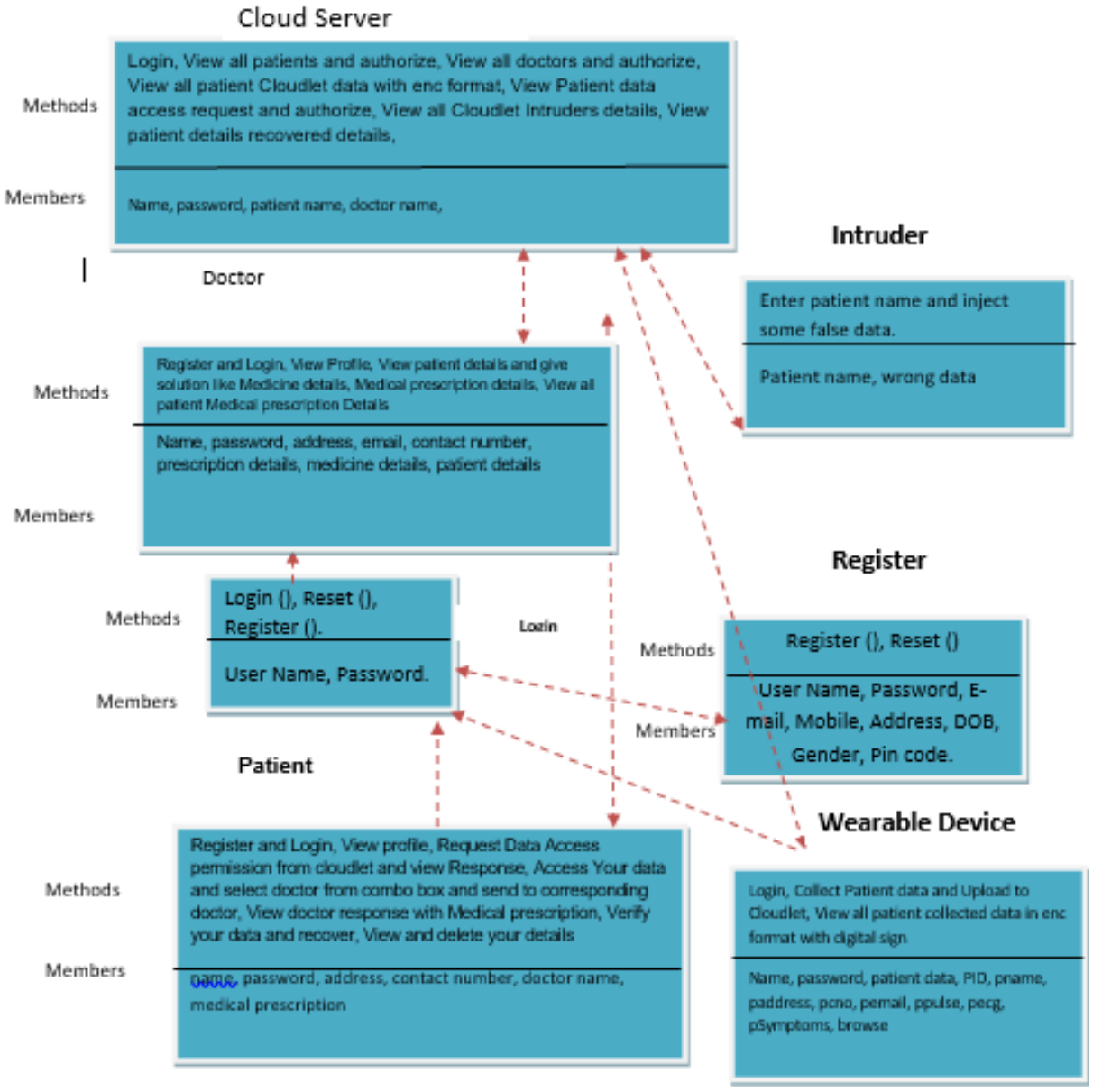

Patient
Request Data Access permission from cloudlet
Access your data and select doctor
View doctor response with Medical prescription
Verify your data and recover and delete your details


Doctor
View patient details and give solution
View patient details and give solution
View all patient Medical prescription Details


Wearable Device
Collect Patient data and Upload to Cloudlet
View all patient collected data in enc format

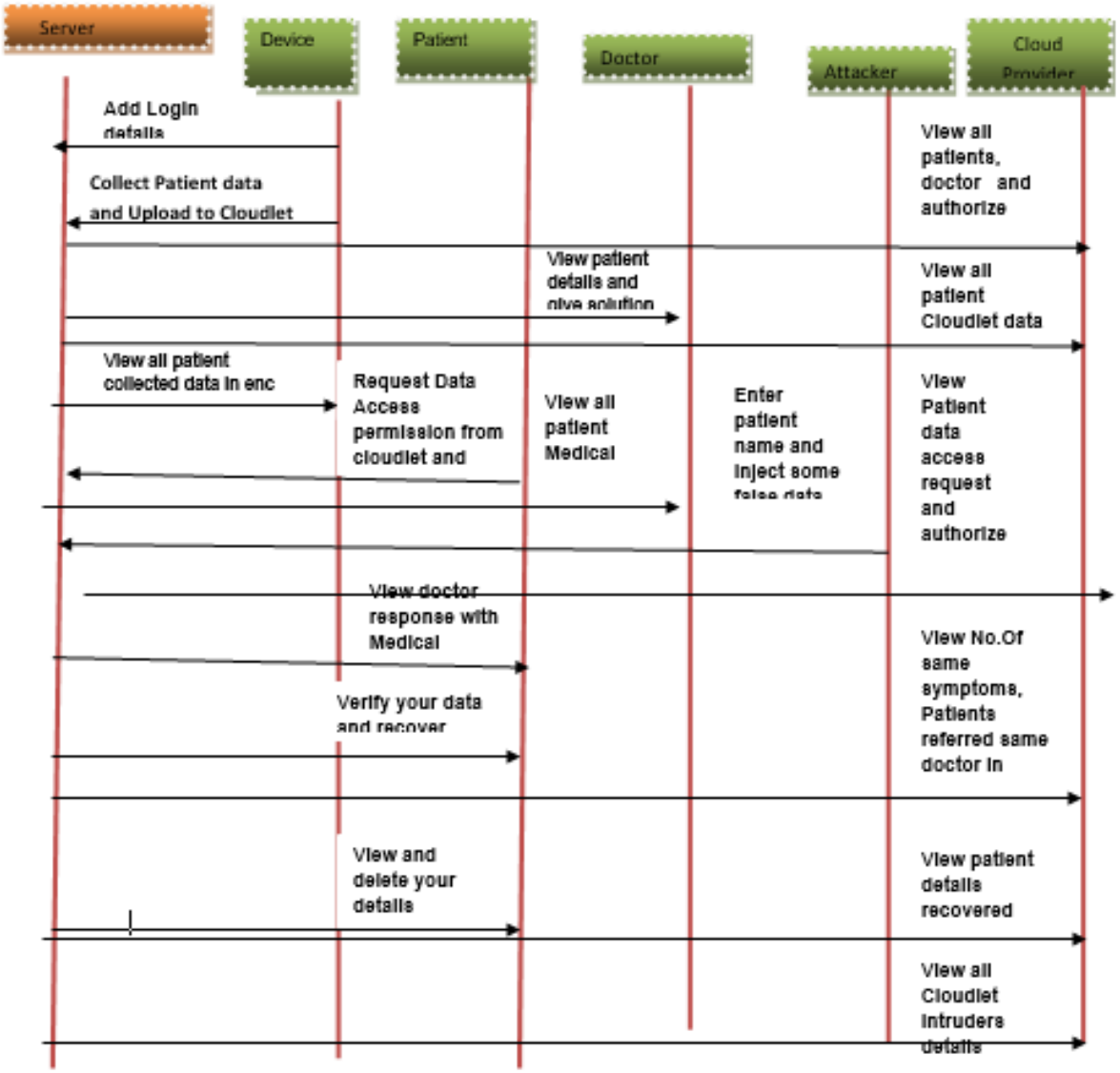
4:6 CLASS DIAGRAM:

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.



4:7 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. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.



CHAPTER 5

IMPLEMENTATION

- Wearable Device

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

- Cloud Server

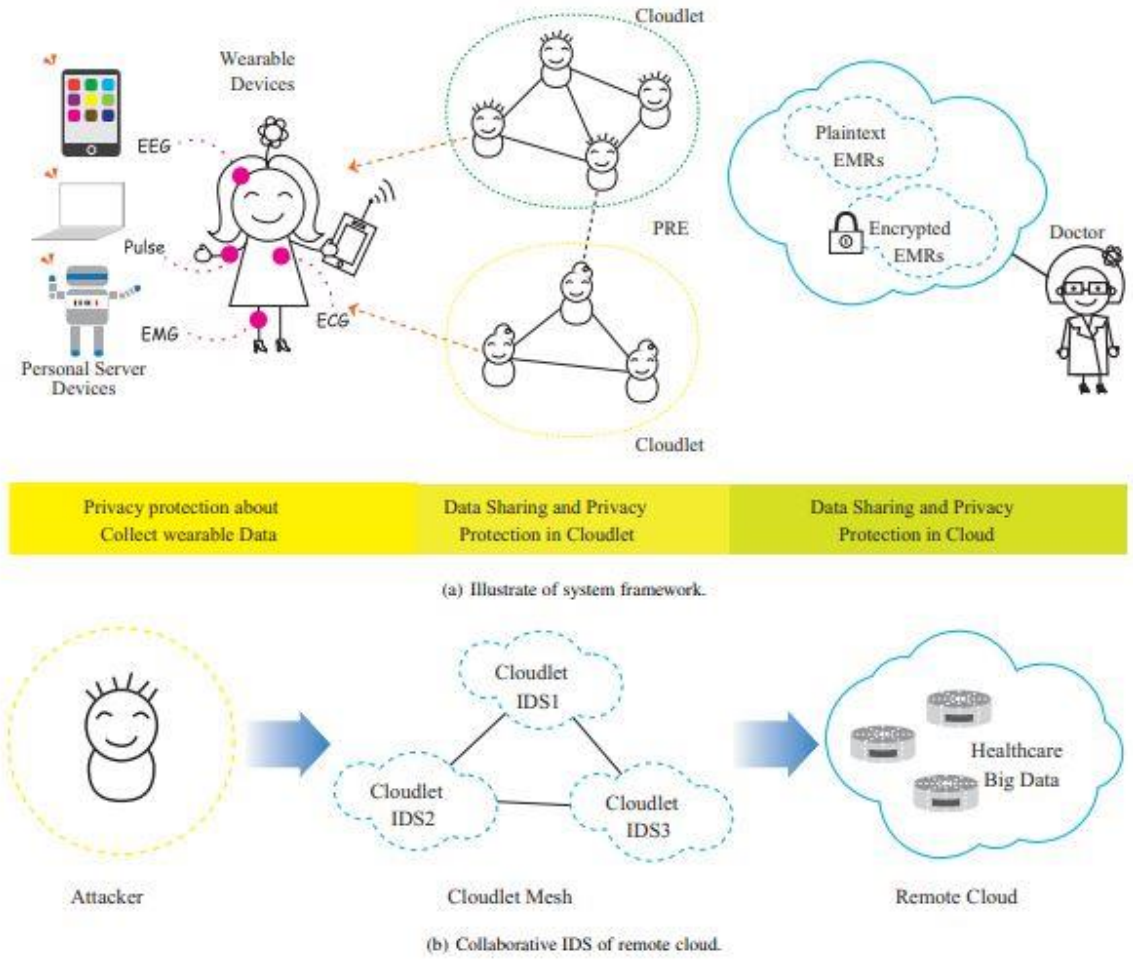
The Cloud server manages which is to provide data storage service for the wearable devices and also View all patients and authorize and View all doctors and authorize ,Vliew all patient Cloudlet data with enc format ,View Patient data access request and authorize ,View all Cloudlet Intruders details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



The framework of the proposed cloudlet-based healthcare system is shown in Fig. 1. The client's physiological data are first collected by wearable devices such as smart clothing [34]. Then, those data are delivered to cloudlet. The following two important problems for healthcare data protection is considered. The first problem is healthcare data privacy protection and sharing data, as shown in Fig. 1(a). The second problem is to develop effective countermeasures to prevent the healthcare database from being intruded from outside, which is shown in Fig. 1(b). We address the first problem on healthcare data encryption an sharing as follows.

• Client data encryption. We utilize the model presented

in [23], and take the advantage of NTRU [35] to protect the

client's physiological data from being leaked or abused.

This scheme is to protect the user's privacy when transmitting the data from the smartphone to the cloudlet.

- Cloudlet based data sharing. Typically, users geographically close to each other connect to the same cloudlet. It's likely for them to share common aspects, for example, patients suffer from similar kind of disease exchange information of treatment and share related data. For this purpose, we use users' similarity and reputation as input data. After we obtain users' trust levels, a certain threshold is set for the comparison. Once reaching or exceeding the threshold, it is considered that the trust between the users is enough for data sharing. Otherwise, the data will not shared with low trust level.

- Remote cloud data privacy protection. Compared to user's daily data in cloudlet, the data stored in remote contain larger scale medical data, e.g., EMR, which will be stored for a long term. We use the methods presented in [36] [21] to divide EMR into explicit identifier (EID), quasi-identifier (QID) and medical information (MI), which will be discussed in 4.3. After classifying, proper protection is given for the data containing users' sensitive information.

- Collaborative IDS based on cloudlet mesh. There is a vast volume of medical data stored in the remote cloud, it is critical to apply security mechanism to protect the database from malicious intrusions. In this paper, we develop specific countermeasures to establish a defense system for the large medical database in the remote cloud storage. Specifically, collaborative IDS based on the cloudlet mesh structure is used to screen any visit to the database as a protection border. If the detection shows a malicious intrusion in advance, the collaborative IDS will fire an alarm and block the visit, and vice-versa. The collaborative IDS, as a guard of the cloud database, can protect a vast number of medical data and make sure o the security of the database.

CHAPTER 7

SOFTWARE TESTING

There are different methods that can be used for software testing. This chapter briefly describes the methods available.

7:1 Black-Box Testing

The technique of testing without having any knowledge of the interior workings of the application is called black-box testing. The tester is oblivious to the system architecture and does not have access to the source code. Typically, while performing a black-box test, a tester will interact with the system's user interface by providing inputs and examining outputs without knowing how and where the inputs are worked upon.

The following table lists the advantages and disadvantages of black-box testing.

Advantages	Disadvantages
Well suited and efficient for large code segments.	Limited coverage, since only a selected number of test scenarios is actually performed.
Code access is not required.	Inefficient testing, due to the fact that the tester only has limited knowledge about an application.
Clearly separates user's perspective from the developer's perspective through visibly defined roles.	Blind coverage, since the tester cannot target specific code segments or errorprone areas.
Large numbers of moderately skilled testers can test the application with no knowledge of implementation, programming language, or operating systems.	The test cases are difficult to design.

7:2 White-Box Testing

White-box testing is the detailed investigation of internal logic and structure of the code. White-box testing is also called **glass testing** or **open-box testing**. In order to perform **white-box** testing on an application, a tester needs to know the internal workings of the code.

The tester needs to have a look inside the source code and find out which unit/chunk of the code is behaving inappropriately.

The following table lists the advantages and disadvantages of white-box testing.

Advantages	Disadvantages
As the tester has knowledge of the source code, it becomes very easy to find out which type of data can help in testing the application effectively.	Due to the fact that a skilled tester is needed to perform white-box testing, the costs are increased.
It helps in optimizing the code.	Sometimes it is impossible to look into every nook and corner to find out hidden errors that may create problems, as many paths will go untested.
Extra lines of code can be removed which can bring in hidden defects.	It is difficult to maintain white-box testing, as it requires specialized tools like code analyzers and debugging tools.
Due to the tester's knowledge about the code, maximum coverage is attained during test scenario writing.	

7:3 Grey-Box Testing

Grey-box testing is a technique to test the application with having a limited knowledge of the internal workings of an application. In software testing, the phrase the more you know, the better carries a lot of weight while testing an application.

Mastering the domain of a system always gives the tester an edge over someone with limited domain knowledge. Unlike black-box testing, where the tester only tests the application's user interface; in grey-box testing, the tester has access to design documents and the database. Having this knowledge, a tester can prepare better test data and test scenarios while making a test plan.

Advantages	Disadvantages
Offers combined benefits of black-box and white-box testing wherever possible.	Since the access to source code is not available, the ability to go over the code and test coverage is limited.
Grey box testers don't rely on the source code; instead they rely on interface definition and functional specifications.	The tests can be redundant if the software designer has already run a test case.
Based on the limited information available, a grey-box tester can design excellent test scenarios especially around communication protocols and data type handling.	Testing every possible input stream is unrealistic because it would take an unreasonable amount of time; therefore, many program paths will go untested.
The test is done from the point of view of the user and not the designer.	

7:4 A Comparison of Testing Methods

The following table lists the points that differentiate black-box testing, grey-box testing, and white-box testing.

Black-Box Testing	Grey-Box Testing	White-Box Testing
The internal workings of an application need not be known.	The tester has limited knowledge of the internal workings of the application.	Tester has full knowledge of the internal workings of the application.
Also known as closed-box testing, data-driven testing, or functional testing.	Also known as translucent testing, as the tester has limited knowledge of the insides of the application.	Also known as clear-box testing, structural testing, or code-based testing.
Performed by end-users and also by testers and developers.	Performed by end-users and also by testers and developers.	Normally done by testers and developers.
Testing is based on external expectations - Internal behavior of the application is unknown.	Testing is done on the basis of high-level database diagrams and data flow diagrams.	Internal workings are fully known and the tester can design test data accordingly.
It is exhaustive and the least time-consuming.	Partly time-consuming and exhaustive.	The most exhaustive and time-consuming type of testing.
Not suited for algorithm testing.	Not suited for algorithm testing.	Suited for algorithm testing.

This can only be done by trial-and-error method.	Data domains and internal boundaries can be tested, if known.	Data domains and internal boundaries can be better tested.

7:5 Levels of Testing

There are different levels during the process of testing. In this chapter, a brief description is provided about these levels.

Levels of testing include different methodologies that can be used while conducting software testing. The main levels of software testing are −

- Functional Testing
- Non-functional Testing

Functional Testing

This is a type of black-box testing that is based on the specifications of the software that is to be tested. The application is tested by providing input and then the results are examined that need to conform to the functionality it was intended for. Functional testing of a software is conducted on a complete, integrated system to evaluate the system's compliance with its specified requirements.

Steps	Description
I	The determination of the functionality that the intended application is meant to perform.
II	The creation of test data based on the specifications of the application.
III	The output based on the test data and the specifications of the application.

IV	The writing of test scenarios and the execution of test cases.
V	The comparison of actual and expected results based on the executed test cases.

There are five steps that are involved while testing an application for functionality.

An effective testing practice will see the above steps applied to the testing policies of every organization and hence it will make sure that the organization maintains the strictest of standards when it comes to software quality.

7:6 Unit Testing

This type of testing is performed by developers before the setup is handed over to the testing team to formally execute the test cases. Unit testing is performed by the respective developers on the individual units of source code assigned areas. The developers use test data that is different from the test data of the quality assurance team.

The goal of unit testing is to isolate each part of the program and show that individual parts are correct in terms of requirements and functionality.

Limitations of Unit Testing

Testing cannot catch each and every bug in an application. It is impossible to evaluate every execution path in every software application. The same is the case with unit testing.

There is a limit to the number of scenarios and test data that a developer can use to verify a source code. After having exhausted all the options, there is no choice but to stop unit testing and merge the code segment with other units.

7:7 Integration Testing

Integration testing is defined as the testing of combined parts of an application to determine if they function correctly. Integration testing can be done in two ways: Bottom-up integration testing and Top-down integration testing.

Sr.No.	Integration Testing Method
1	**Bottom-up integration** This testing begins with unit testing, followed by tests of progressively higher-level combinations of units called modules or builds.
2	**Top-down integration** In this testing, the highest-level modules are tested first and progressively, lower-level modules are tested thereafter.

In a comprehensive software development environment, bottom-up testing is usually done first, followed by top-down testing. The process concludes with multiple tests of the complete application, preferably in scenarios designed to mimic actual situations.

7:8 System Testing

System testing tests the system as a whole. Once all the components are integrated, the application as a whole is tested rigorously to see that it meets the specified Quality Standards. This type of testing is performed by a specialized testing team.

System testing is important because of the following reasons −

- System testing is the first step in the Software Development Life Cycle, where the application is tested as a whole.
- The application is tested thoroughly to verify that it meets the functional and technical specifications.
- The application is tested in an environment that is very close to the production environment where the application will be deployed.
- System testing enables us to test, verify, and validate both the business requirements as well as the application architecture.

7:9 Regression Testing

Whenever a change in a software application is made, it is quite possible that other areas within the application have been affected by this change. Regression testing is performed to verify that a fixed bug hasn't resulted in another functionality or business rule violation. The intent of regression testing is to ensure that a change, such as a bug fix should not result in another fault being uncovered in the application.

Regression testing is important because of the following reasons −

- Minimize the gaps in testing when an application with changes made has to be tested.
- Testing the new changes to verify that the changes made did not affect any other area of the application.
- Mitigates risks when regression testing is performed on the application.
- Test coverage is increased without compromising timelines.
- Increase speed to market the product.

7:10 Acceptance Testing

This is arguably the most important type of testing, as it is conducted by the Quality Assurance Team who will gauge whether the application meets the intended specifications and satisfies the client's requirement. The QA team will have a set of pre-written scenarios and test cases that will be used to test the application.

More ideas will be shared about the application and more tests can be performed on it to gauge its accuracy and the reasons why the project was initiated. Acceptance tests are not only intended to point out simple spelling mistakes, cosmetic errors, or interface gaps, but also to point out any bugs in the application that will result in system crashes or major errors in the application.

CHAPTER 8

CONCLUSION

In this project, 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 well as low communication cost. However, it does allow users to transmit data to a cloudlet, which triggers 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-preserving of 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.

CHAPTER 9

BIBLOGRAPHY

[1] K. Hung, Y. Zhang, and B. Tai, “Wearable medical devices for telehome 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.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy preserving multi-keyword ranked

search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[12] K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.

[13] T. Xu, W. Xiang, Q. Guo, and L. Mo, "Mining cloud 3d video data for interactive video services," Mobile Networks and Applications, vol. 20,no. 3, pp. 320–327, 2015.

[14] M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.

[15] K. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.