A Project Report

on

"E-LEARNING ON CLOUD USING ADVANCED ENCRYPTION STANDARD"

Submitted to the

Savitribai Phule Pune University

In partial fulfilment for the award of the Degree of

Bachelor of Engineering

in

Information Technology

by

Yash Pawar

Vaibhavi Pawar

Pranali Wagh

Abhishek Pujari

Under the guidance of

Dr.Mrs.K.S.Thakare

Sinhgad Institutes

Department of Information Technology

STES's Sinhgad College of Engineering

Vadgaon (Bk.), Off. Sinhgad Road,

Pune 411041.

2019-2020

Sinhgad Institutes

CERTIFICATE

This is to certify that the project report entitled

"E-LEARNING ON CLOUD USING ADVANCED ENCRYPTION STANDARD"

submitted by

Yash Pawar

Vaibhavi Pawar

Abhishek Pujari

Pranali Wagh

is a bona fide work carried out by them under the supervision and guidance of Dr. Mrs.K.S.Thakare and it is approved for the partial fulfilment of the requirement of Savitribai Phule Pune University for the award of the Degree of Bachelor of Engineering(Information Technology)

This project report has not been earlier submitted to any other Institute or University for the award of any Degree or Diploma.

Dr.Mrs.K.S.Thakare
Internal Guide

Prof. G. R. Pathak
Head of the Department

External Examiner

Dr. S. D. Lokhande
Principal

Date:
Place: Pune

This Project Based report has been examined by us as per the Savitribai Phule Pune University, Pune requirements at STES's Sinhgad College of Engineering, Pune-411041 on . . . . . .

Internal Examiner

External Examiner

ACKNOWLEDGMENT

I am highly indebted to my guide Dr. Mrs. K. S. Thakare for her guidance and constant supervision as well as for providing necessary information regarding the project report and also for her support in completing the Project report. I would like to express my special gratitude and thanks to Staff Members of department of Information Technology for giving me such attention and time.

This acknowledgment would be incomplete without expressing my thanks to Prof. G. R. Pathak, Head of the Department (Information Technology) for his support during the work.

I would like to extend my heartfelt gratitude to my Principal, Dr. S. D. Lokhande who provided a lot of valuable support, mostly being behind the veils of college bureaucracy.

I would also like to express my gratitude towards my parents and friends for their kind co-operation and encouragement which help me in completion of this report. My thanks and appreciations also go to my colleague in developing the seminar report and people who have willingly helped me out with their abilities.

(Yash Pawar) (Vaibhavi Pawar)

(Abhishek Pujari) (Pranali Wagh)

Contents

List of Figures

Abstract

Various benefits of Information Technology have created different tools that help learning at any place and anytime. As the technology is changing, education system also needs to be changed for faster, comfortable and easy learning. Information Technology has been involved in learning process which is known as e- learning. Nowadays it is also called as modern learning. Various devices need to use this technology efficiently and its importance. Various devices need the driver and a communication device which may be difficult to use and costly.

Various computer features and services has been revolutionized by cloud computing where various resources are offered as a service over the internet. The basic three services provided by cloud are Software as a service (SaaS), Platform as a service (PaaS), Infrastructure as a service (IaaS). Application model of Hybrid Cloud has various advantages such as elastic computing resources, safety, privacy and cost effectiveness.

Chapter 1

Introduction To Project Topic

1.1 Introduction

The term Cloud refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Cloud can provide services over public and private networks, i.e., WAN, LAN or VPN. Now a day's E-learning is becoming popular in the educational field. E-learning adapts the use of computers and networks to improve the quality of education. The motive of E-learning is to allow the student to learn independently at any place at any time**.** Education is usually perceived as the method whereby we have students in a classroom receiving lessons from a Teacher but with the help of IT through the internet, learning can now be achieved without necessarily having a teacher right in front of a student. E-learning is one of the tools that emerged from IT & has been integrated into many university educational programs, shifting from the traditional way of education to electronic environment in which a student can access & make use of information anywhere and at any convenient time**.**

The modern advances in Information and Communication technologies enable us to work and study from a distance. It is widely perceived that learning can happen outside the classroom. It also seems impossible to find institutions in higher education that don't offer opportunities for remote online learning. In order to evaluate the skills, knowledge, or attitudes of students, education material is required to the student. Different types of study material will upload by teachers depends on the student requirement, for example, the Video or text document or image will help to Learners measure their own. E-learning provides infrastructure based on modern methodologies and tools

1.2 Motivation behind E-learning on cloud using advanced encryption standard

Today Engineering students are highly dependent on the internet for browsing ,that may be study related material or any other information they are sometimes confused on what is the exact information they just keep on redirecting to different pages for information, for this purpose a web based application on cloud will help them to access as well as download the data according to their requirements.

1.3 RELEVANCE

The aim is to develop an e-learning system that will improvise on the traditional learning, large class learning techniques used in teaching. To design an e-learning system with various multimedia features like text, images, videos, audios. To create a database for easy retrieval, storage & maintenance of student records as well as sharing of data between users. To create a user-friendly frontend design that will be linked to a database for information retrieval. To make the training process easier for the trainer as well for uploading materials using Advanced Encryption Standard and for a key generation we are using ECC Algorithm. To propose and to implement the improved e-learning system that provides content services to the provision and sharing of various forms of educational content, including text, images, videos, 3D objects and scenes of virtual reality and augmented reality.

1.4 Aim and Objective(s) of the work

The aim is to develop an e-learning system that will improvise on the traditional learning, large class learning techniques used in teaching. To design an e-learning system with various multimedia features like text, images, videos, audios. To create a database for easy retrieval, storage & maintenance of student records as well as sharing of data between users. To create a user-friendly frontend design that will be linked to a database for information retrieval. To make the training process easier for the trainer as well for uploading materials using Advanced Encryption Standard and for a key generation we are using ECC Algorithm. To propose and to implement the improved e-learning system that provides content services to the provision and sharing of various forms of educational content, including text, images, videos, 3D objects and scenes of virtual reality and augmented reality.

Project Objectives:

1. Enhance the quality of learning and teaching.
2. Meet the learning style or needs of students.
3. Improve efficiency and effectiveness.
4. Improve user-accessibility and time flexibility to engage learners in the learning process.

1.5 Problem Statement

To propose and to implement the improved e-learning system that provides content services to the provision and sharing of various forms of educational content, including text, images, videos, 3D objects and scenes of virtual reality and augmented reality.

Chapter 2

Literature Survey

1. Mohsen Maraoui, et al developed at **"Smart Tools for Cloud E-learning System"**

Author tries a new and innovative solution for media services that can be accessed from smart devices cloud-based intelligent service environment with a fully integrated system. Indexation has been used. It can be utilized under circumstances where the availability of resources is limited Post problems related to searching are tedious, costly in resources and time.

2. Miri Barak et al developed "**On-campus or online: examining self regulation and cognitive transfer skills in different learning settings"**

Author set to recognize self-regulation skills necessary for online education and to illustrate cognitive move of on-campus and online students. The study integrated two groups of undergraduate students who studied the same course. They are used Self-regulated learning (SRL), diverse learning. Students pointed out that learning from a distance gives them flexibility With respect to time.
The study was conducted in one higher education institution with a relatively small number of participant's eighty-four science and engineering students.

3. Haibo Yi et al developed "**Implementation of Learning Management System Based on Cloud Computing"**

The author has used basic services of cloud like SaaS providing various software like learning system, examination system, PaaS providing on platform software like MySQL, Cfree, oracle, IaaS for providing different kinds of services in this learning model on open stack cloud computing systems using Microsoft ASP.net and SQL .1.Efficient model 2.On demand computer resources sharing. Integrating these services is difficult.

4. Seppo J. Sirkemaa et al developed **"Analysing e-Learning and Modern Learning Environments "**

E-learning makes it possible to study regardless of time and space. It may also provide new groups of student's opportunities that are not available with other forms of education. They are using Traditional storage algorithm. 1. Helps in meeting new 2.People exchanging ideas between individual students and student groups . e-learning has failed to satisfy the needs of a mobile user.

5. Abiodun Kilanko et al developed " **E-learning on the Cloud – An Analysis"**

Cloud providers have platform for users to design and run application located in the cloud. E-learning provides a web based forum for students. Computing power and storage are also being provides on the cloud.These provisions available on the cloud makes it most suitable for e-learning purpose.

6. Qasim Alajmi et al developed **" E-Learning Models: The Effectiveness of the Cloud Based E-Learning Model over the Traditional ELearning Model ".**

This paper understand the effectiveness of the traditional and cloud-based e-learning model. E-learning model is the best learning model for individuals learning from home and for education providers as well. Internet has made it easy to for learners and educators to share information interactively, which is vital in enhancing education.

7. Dr. Birajkumar V. Patel "**Implementation of Cloud Computing(Software as a Service) for Product based Search Engine"**

There are many search engines available on the web. All are providing solutions in the form of list of URLs, text,images, videos, etc. The new model allow user to get domain specific and decision making information based on past transactions stored. Designing new model incorporates optimizing business strategies for future survival of business

BACKGROUND

The aim is to develop an e-learning system that will improvise on the traditional learning, large class learning techniques used in teaching. To design an e-learning system with various multimedia features like text, images, videos, audios. To create a database for easy retrieval, storage & maintenance of student records as well as sharing of data between users. To create a user-friendly frontend design that will be linked to a database for information retrieval. To make the training process easier for the trainer as well for uploading materials using Advanced Encryption Standard and for a key generation we are using ECC Algorithm. To propose and to implement the improved e-learning system that provides content services to the provision and sharing of various forms of educational content, including text, images, videos, 3D objects and scenes of virtual reality and augmented reality

Chapter 3

System Requirements

3.1 Software requirements:

- Java: jdk 1.6 or above
- IDE: Eclipse (Oxygen)
- Server: Apache Tomcat 7 or 8
- Database: MySQL Server8.0

3.2 Hardware requirements:

- Processor: Pentium –IV
- RAM: 2 GB (min)
- Hard Disk: 20 GB
- Cloud :Amazon Web Services(AWS S3)

Functional Requirements

User Environment

• The application will be used on computer based on Windows Operating System.

• Platform used will be Java, where we used JDK1.8 as developing environment.

• Front end Java Swings and backend is MySQL 5.7.19 database.

• SQL jar are the External API that we used in our development cycle.

Operating Environment

The Proposed System Supports

• OS: Windows XP, Windows 10

• Database: MySQL

Software Requirement

- Platform: JAVA
- Technology: JDK 1.8
- Database: MySQL
- IDE: Eclipse
- Server: Apache Tomcat 8.
- Web Front End: JSP pages

Performance Requirements

For good performance, the server should be indicated only to local host and most of the RAM should be used for our application. Good internet bandwidth for mail sending so the API server can handle more requests at a time.

Safety Requirements and Security

For the safety purpose backup of the database must be required. For the security purposes and to avoid illegal use of the system, while using this application user must do the following things:
At first, the user has to register to the system.

There are four security requirements
a. Secure Functional Requirements- this is a security related description that is integrated into each functional requirement. Typically, this also says what shall not happen. This requirement artifact can for example be derived from misuse cases.
b. Functional Security Requirements- these are security services that need to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations.
c. Non-Functional Security Requirements- these are security related architectural requirements, like \robustness\minimal performance and scalability". This requirement type is typically derived from architectural principals and good practice standards.
d. Secure Development Requirements- these requirements describe required activities during system development which assure that the outcome is not subject to vulnerabilities. Examples could be data classification \coding guidelines or test methodology.

Software Quality Attributes:

- Availability: The system should be available 24 * 7 provided the internet connection is available.

- Correctness: The system should suggest accurate disease when given with the required parameter values. System is planned in such a way that it will give the most correct output.
- Reliability: The system should support all platform and update within time.
- Reusable: This software is reusable.
- Portable: As software is a mobile camera based it automatically introduces portability.
- Also, the system satisfies other quality attributes such as interoperability, maintainability and edibility.

Chapter 4

Design

4.1 System Design

The user will first login to the system. If the user does not have login, then (s)he has to register first and then can login to the system further. The data owner (Teacher) who stores private data in the cloud (by different categories), and allows the data consumer to access his private data (of some category) from the cloud. The cloud is an entity that provides storage services and is responsible to help the data owner (Teacher) to distribute the private data (belonging to some particular category) to the data consumer (Student). The student is an entity who first gets data access permission (of some data category) from the teacher (and this only happens once per data category), and then access the data owner's private data from the cloud.

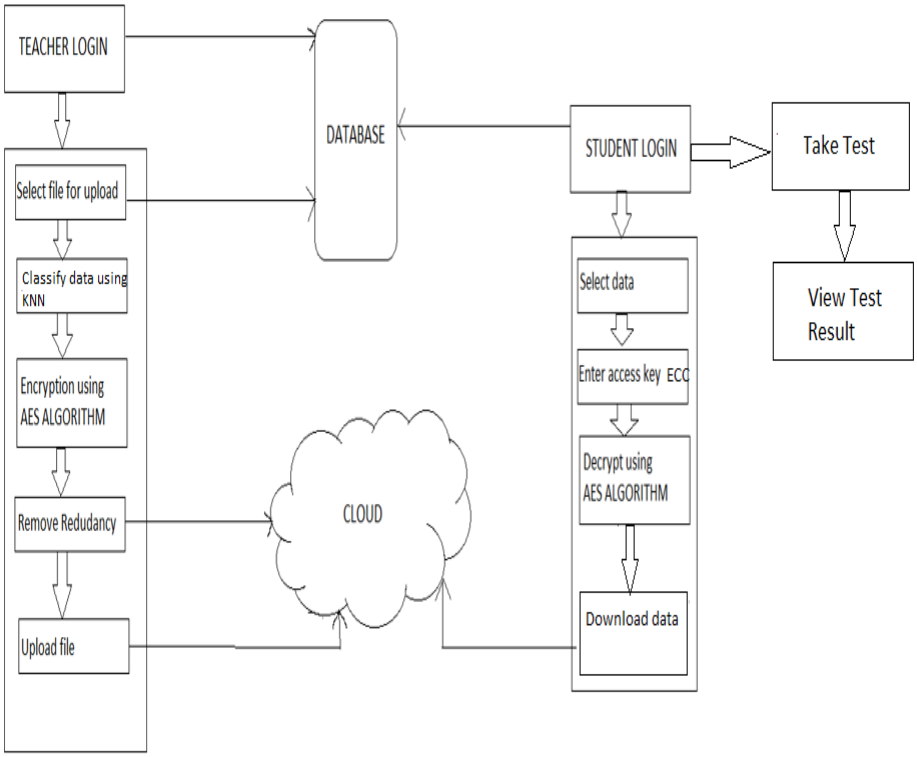


Figure 7.1: System Architecture

4.2 Data Flow Diagrams

DFD 0

This is initial Data Flow Diagrams in this diagrams we are show only initial design like User Data, System, Database. Here User Data is supporting System and System is our Main System and Database is used for storage

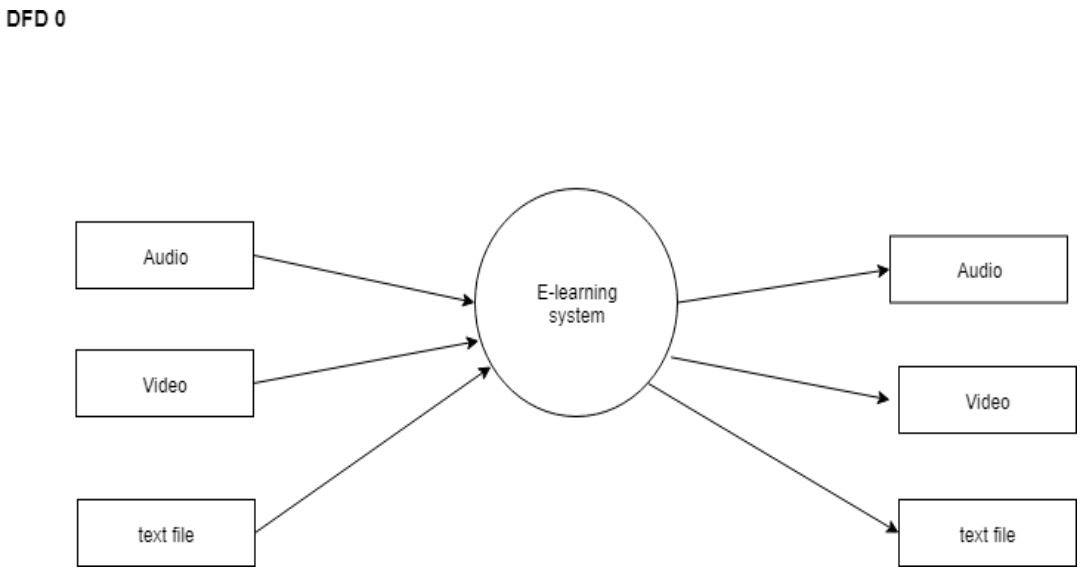


Figure 7.2: DFD 0

DFD 1

Student This is Data Flow Diagrams 1 in this diagrams 50 to 60 % design all the functionality of user and owner module is shown

DFD-1 Student Diagram

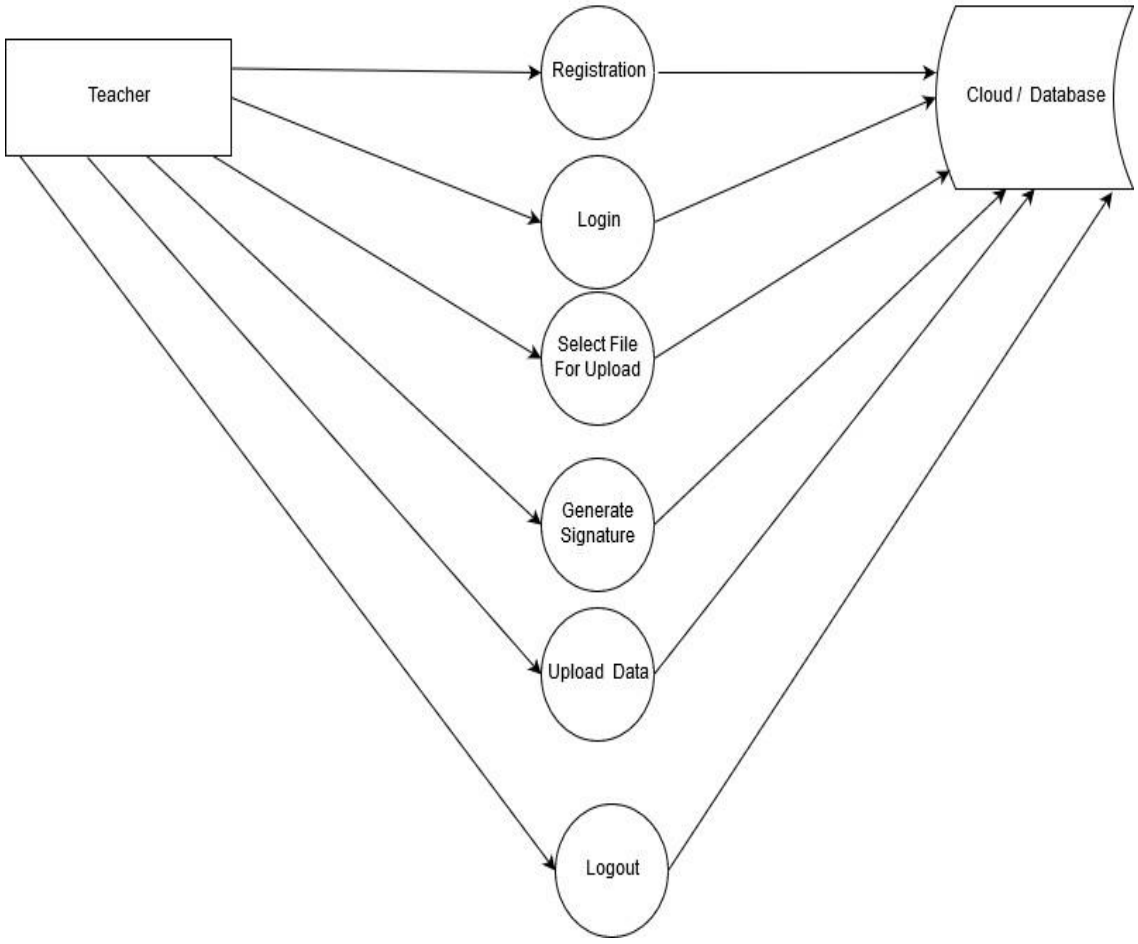


Figure 7.3: DFD 1

DFD 2

Student This is Data Flow Diagrams 2 in this diagram we are showing 100 % design of our system like all the functionality of user and owner module.

Figure 7.4: DFD 2

4.3 UML Diagrams

Use Case Diagram

Use case diagram is a representation of a user's interaction with the system that shows relationship between the user and the different use cases in which the user is involved.

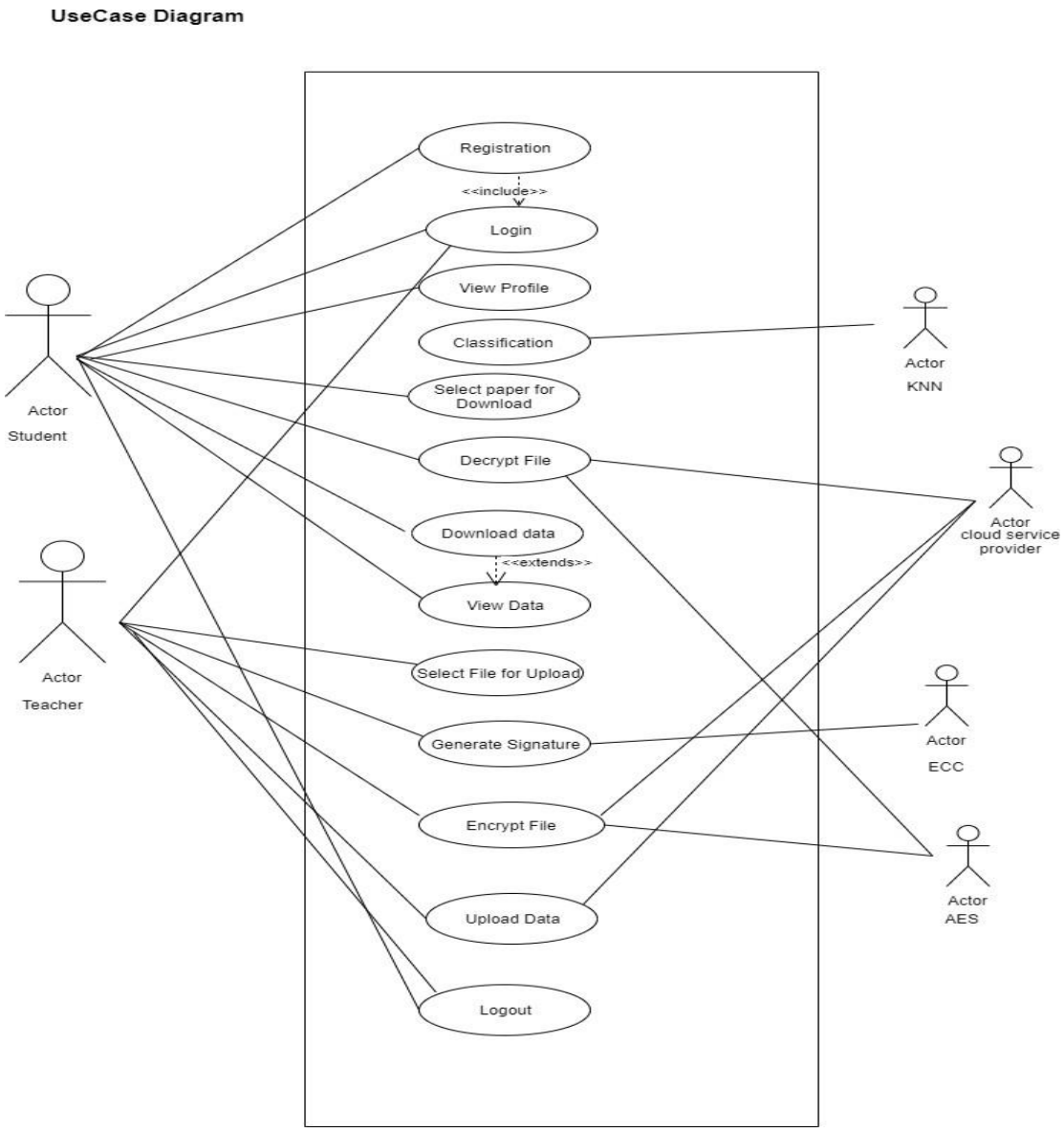


Figure 7.5: Use Case

Sequence diagram: Sequence diagram is a representation of ordered actions in the system that shows relationship between the user and the different use cases in which the user is involved.

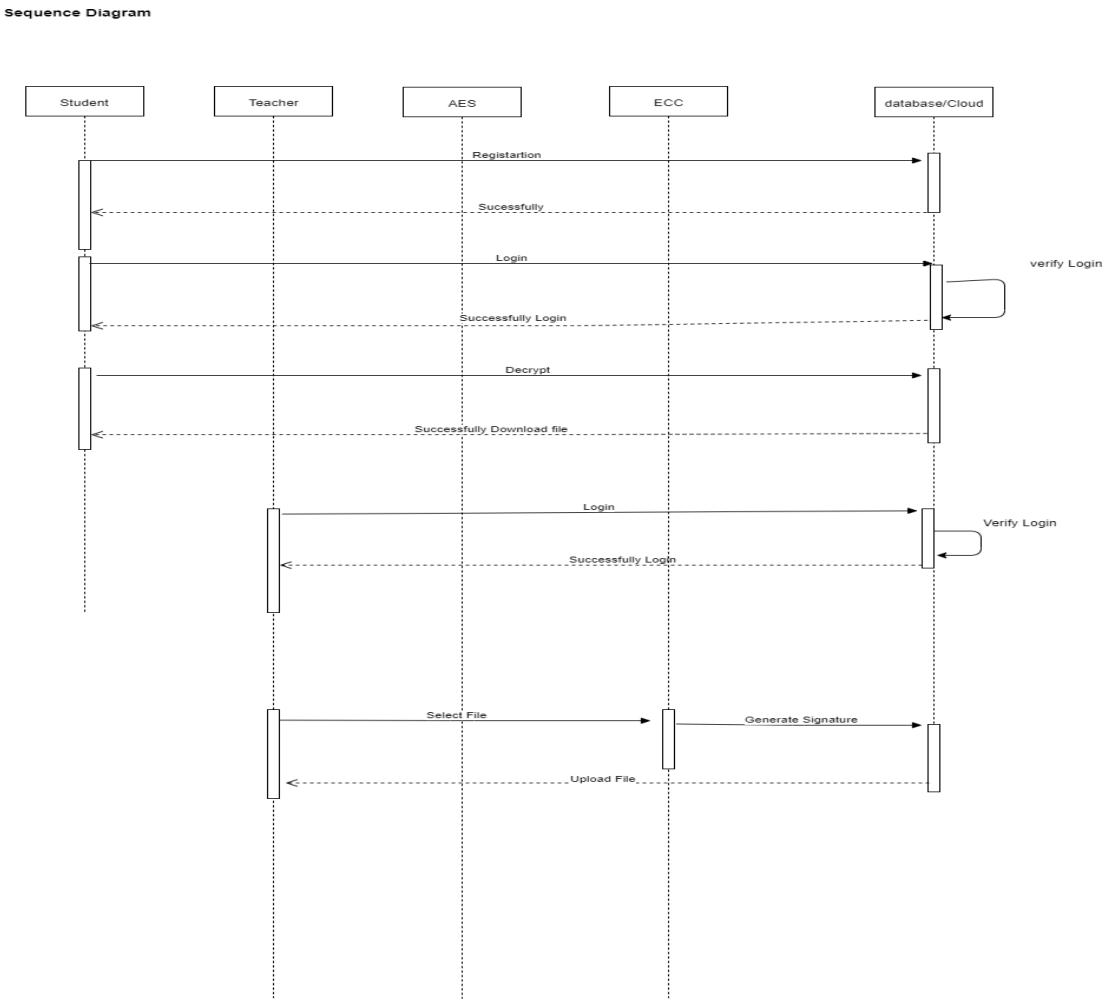


Figure 7.6: Sequence Diagram

Class diagram: Class diagram describes the structure of a system by showing the systems classes, their attributes, operations and relationships among objects.

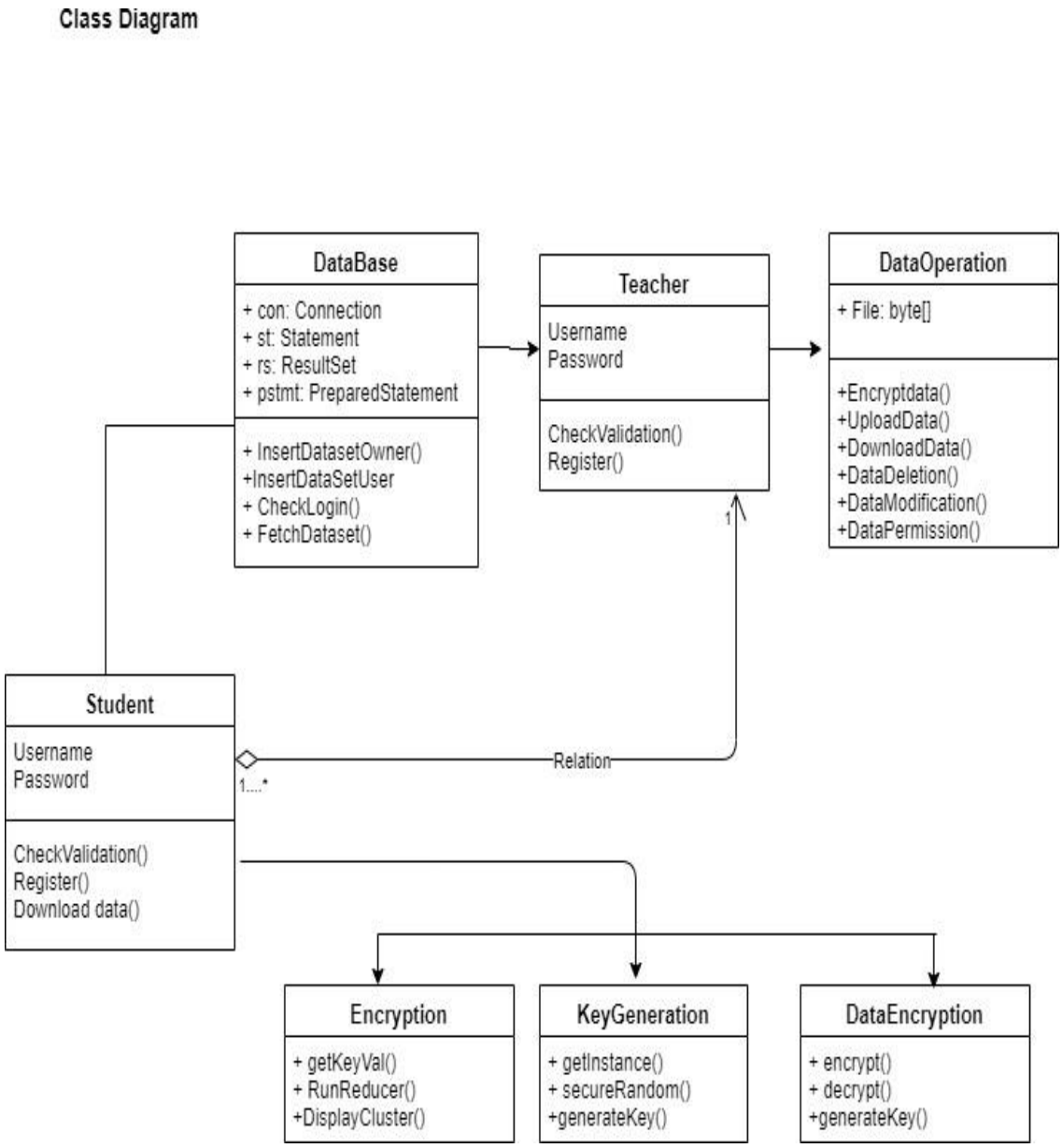


Figure 7.7: Class Diagram

Deployment diagram: Deployment diagram shows the execution architecture of a system,including nodes such as hardware or software execution environments ans middleware connecting them.

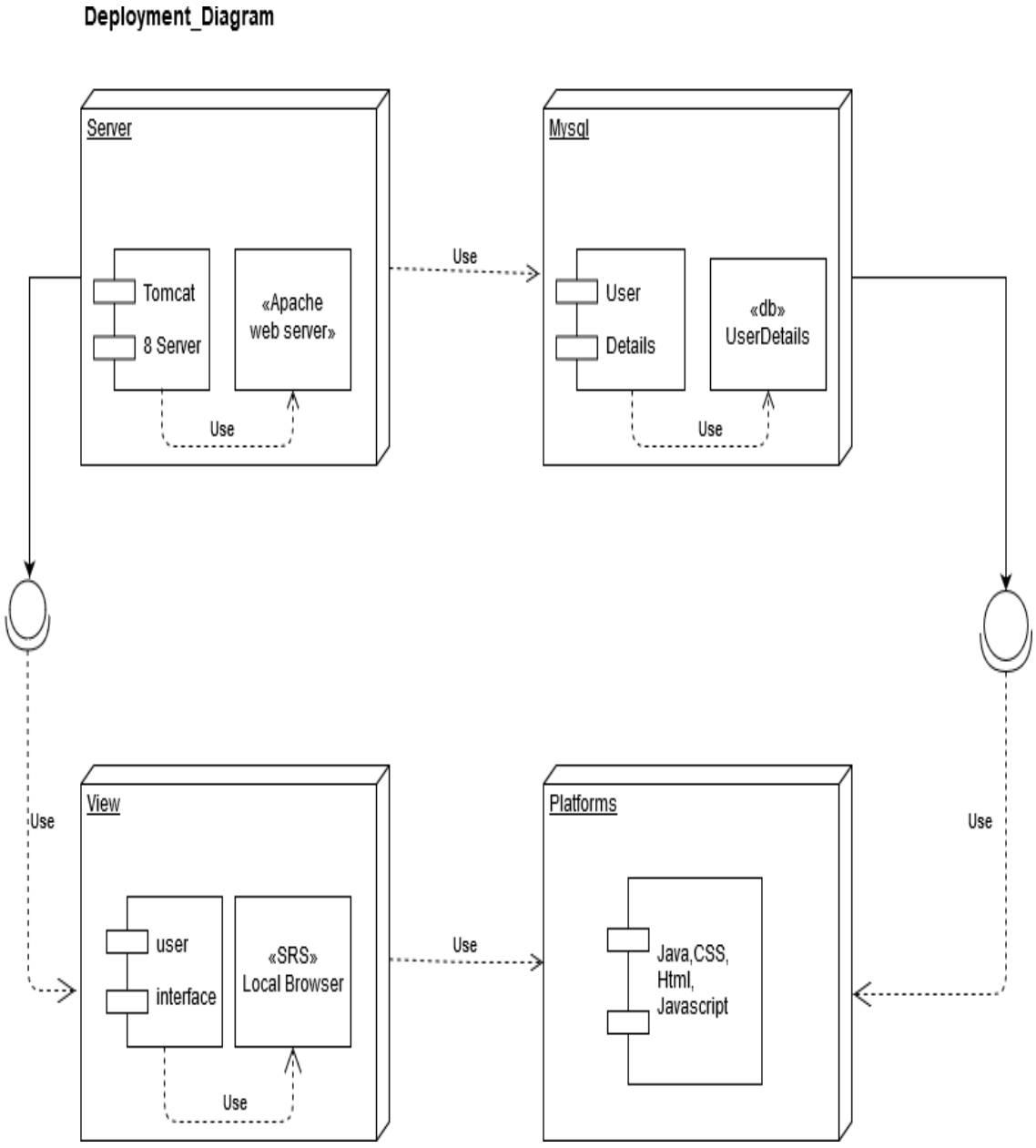


Figure 7.8: Deployment Diagram

IMPLEMENTATION

Planning:

Requirements: In this phase of our project we have gathered all the requirements which helps in finding out exact need of user as well as the service provider.

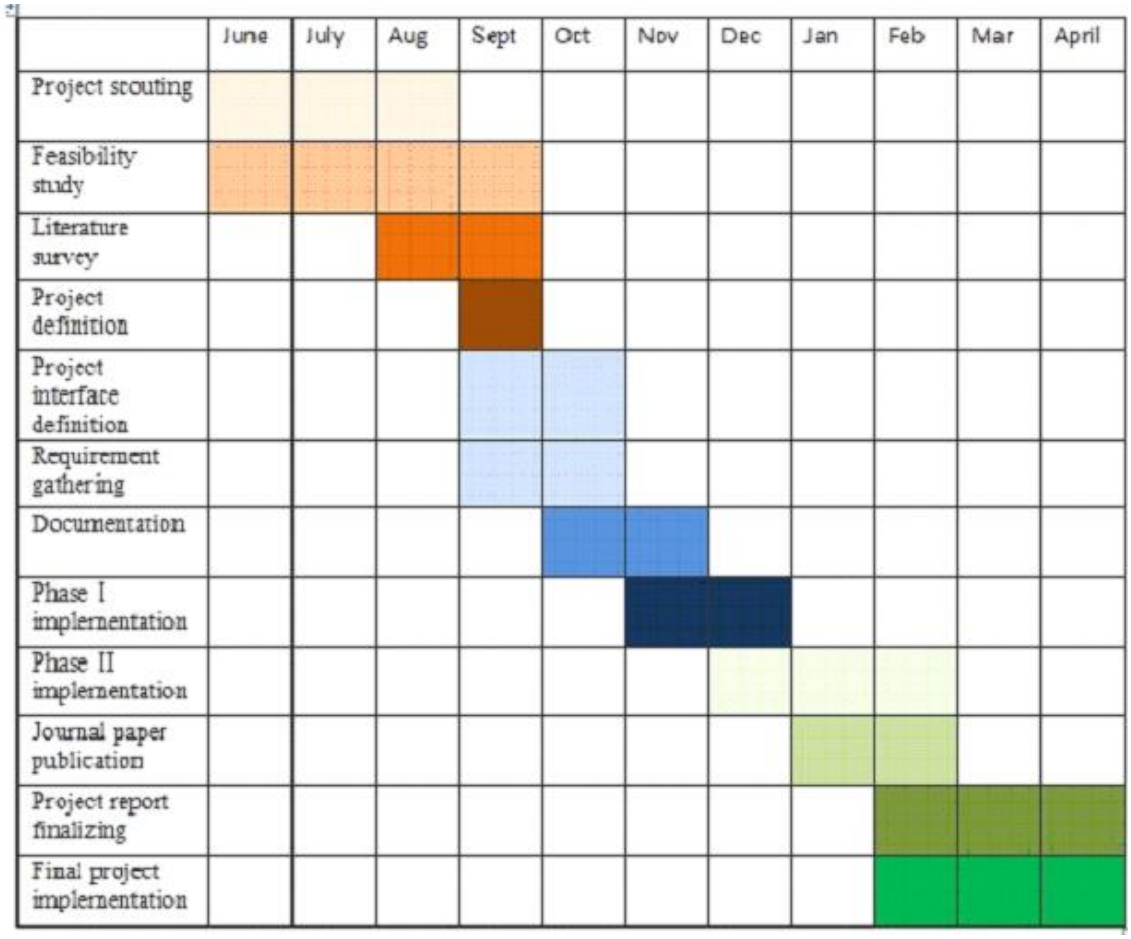
System Design: Helps in specifying hardware and system requirements and helps in defining overall system architecture.

Coding: In this phase, we will start the actual coding. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

Integration and Testing: In this phase, all the units developed in the coding phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.

Deployment Phase: In this phase, once the functional and nonfunctional testing is done, the product is deployed in the customer environment or released into the market.

Maintenance: In this phase, some issues which come up in the client environment. To fix those issues patches are released. Also, to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment



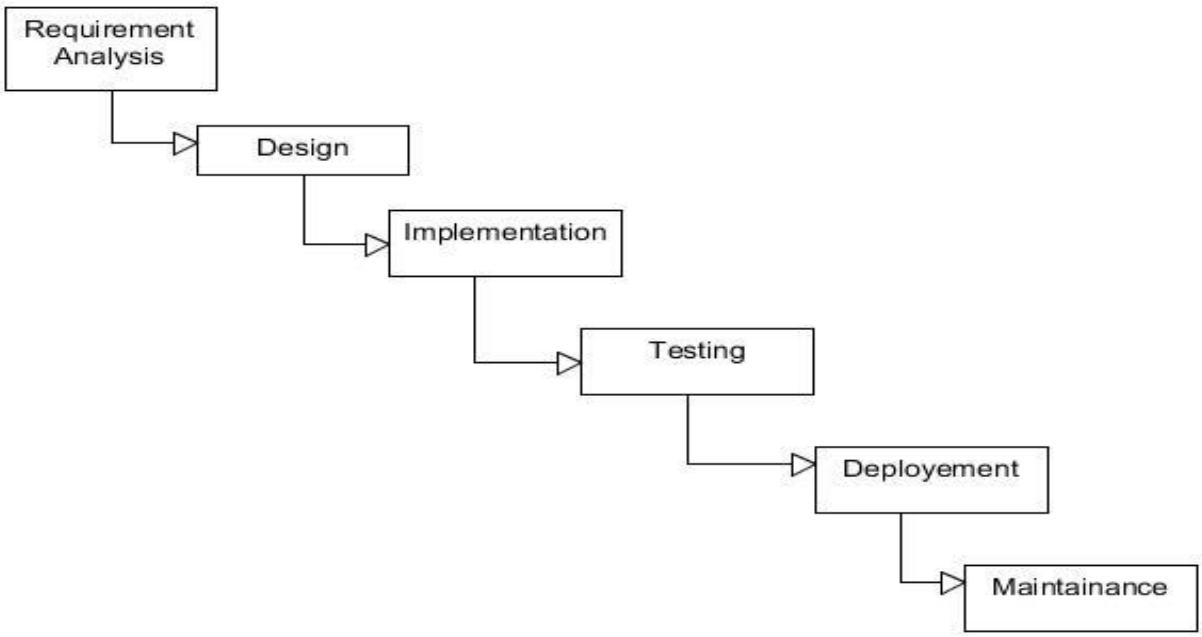
Project Task Set

Major Tasks in the Project stages are:

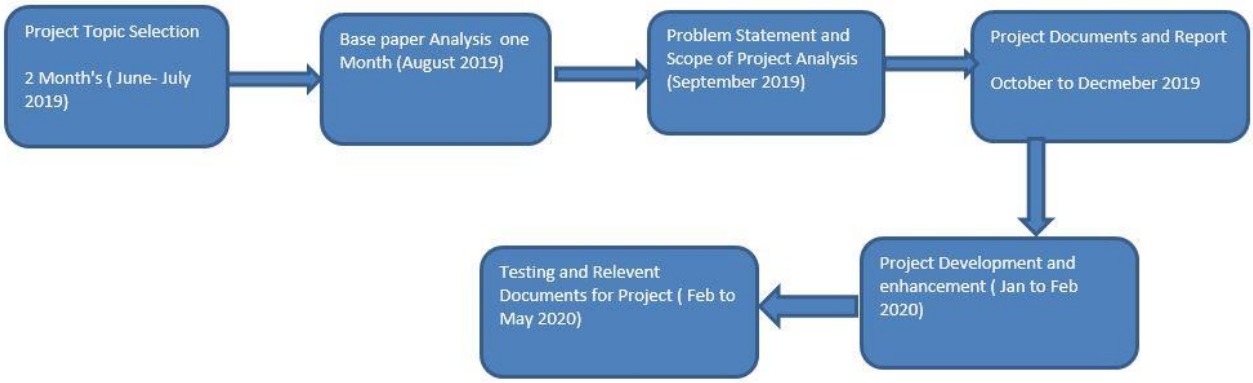
- Task 1: The First task in our project was to search the topic. We need to search for the project which is practically oriented and theoretically aligned. After reading all the description and discussing it with others a project topic is finalized.

- Task 2: After finalizing with others, our next task is to identify the problem. Problem identification involves a lot of background work in the general area of the problem. Normally it calls for the use of prior experience, typically experience we may not yet have. For identifying the task, we need to read as much base paper as we can.

- Task 3: After identifying the problem we are now able to design our system. For designing we are using UML diagrams methodology. We will design our system to achieve the technical feasibility. After designing we have analysed our design to ensure it meets the specifications.
- Task 4: After the designing is finalized we now start with the actual coding part. We will split the coding into small modules. When each module is fully qualified, we will integrate into one system.
- Task 5: After the implementation of our idea, we must test for the bugs by using all possible test scenarios and test cases.
- Task 6: After the testing phase is done, we are now ready to deploy our project.



Software Development Life Cycle



Timeline Chart

Graphical User Interface (GUI) SNAPSHOTS

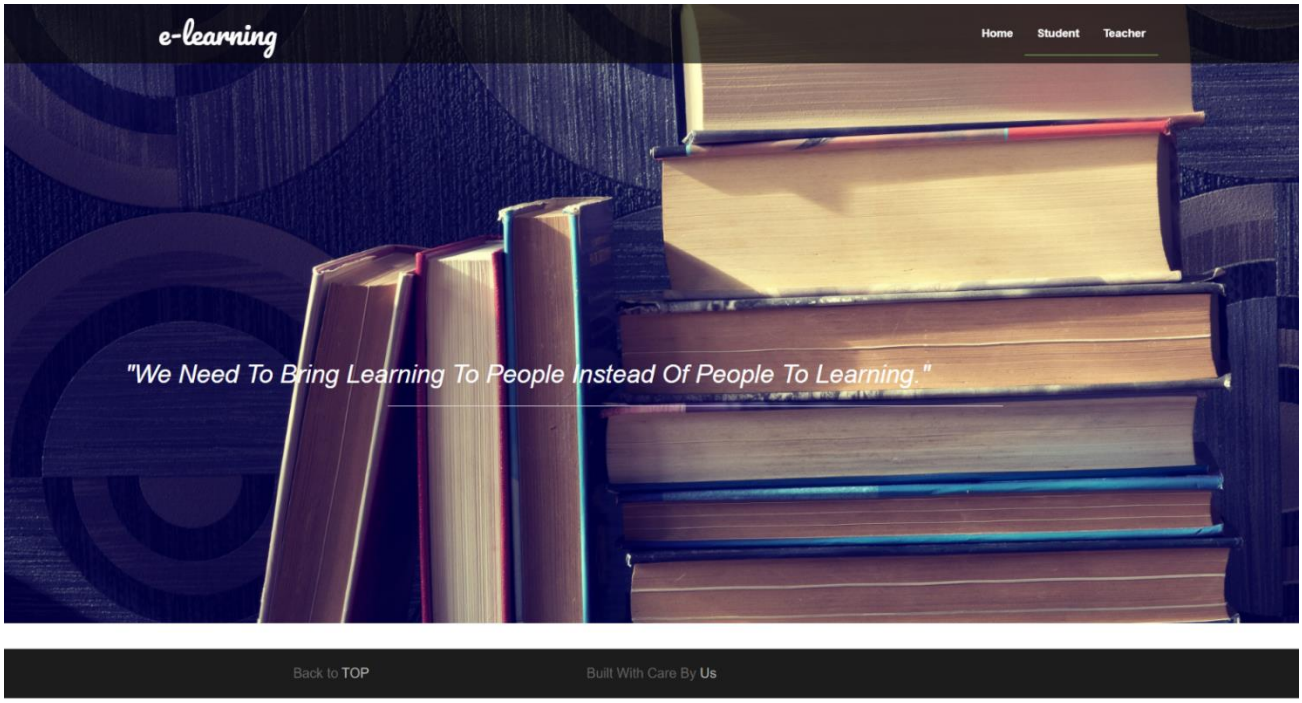


Fig 8: Home Page

This is the home page of our project which contains the student section and teacher section which contain individual functionality.

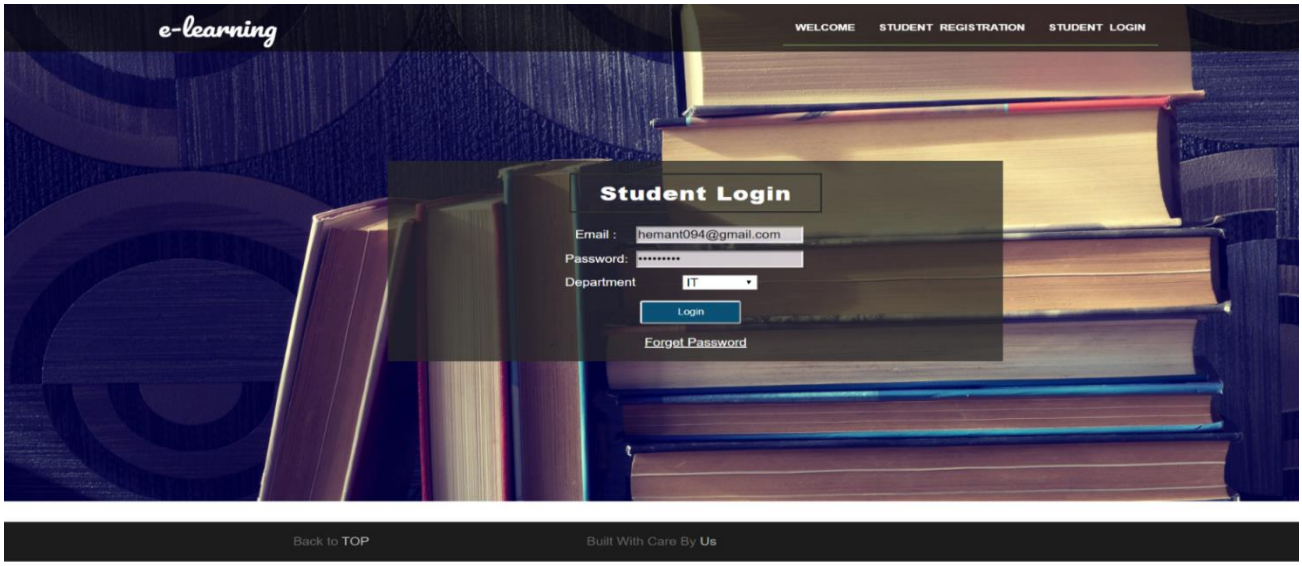


Fig 9: Student Login Page

This is Student login page where student can login through email and password. validations have been used for real life approach.

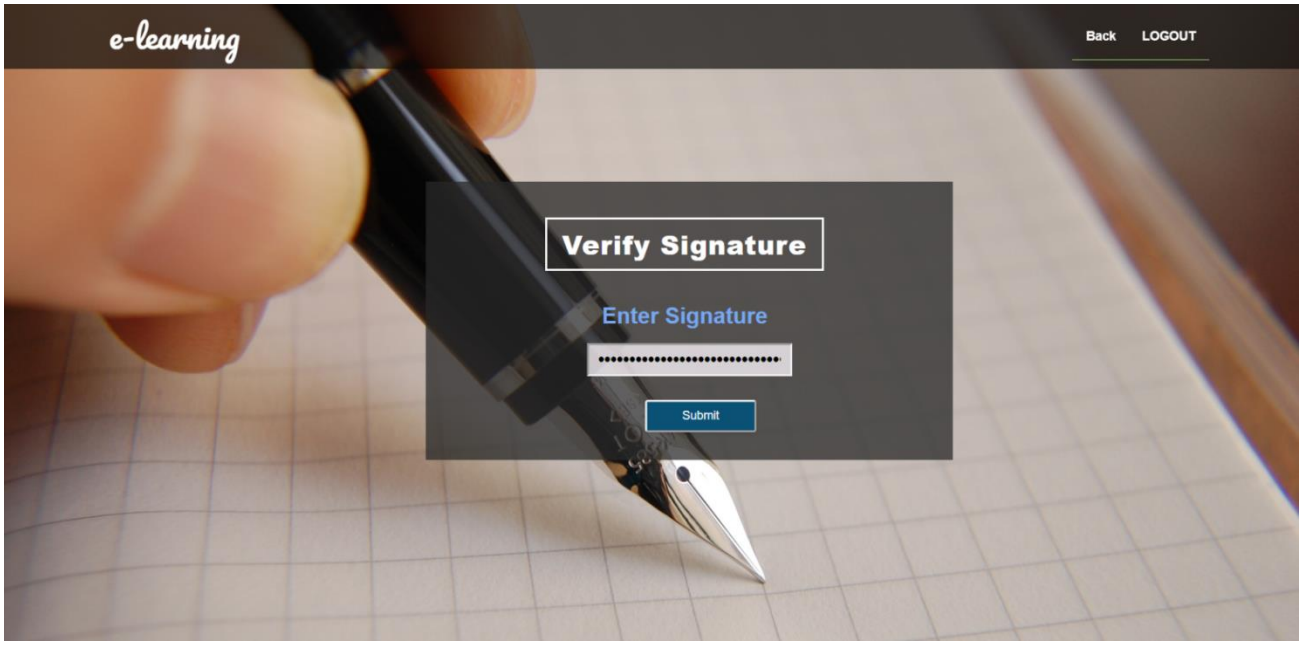


Fig 10: ECC Signature Verification

This page is used to take the Signature provided to student once he tried to login. This signature is created by ECC algorithm.

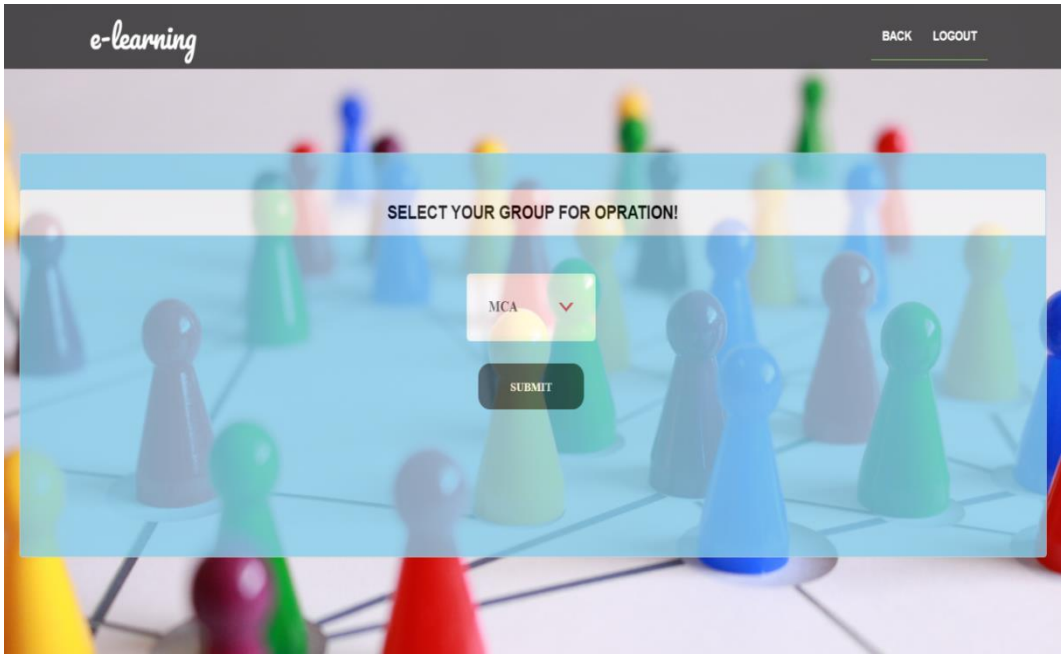


Fig 11: Student Category Page

This page is used to differentiate different types of students so that they can access their own study material.

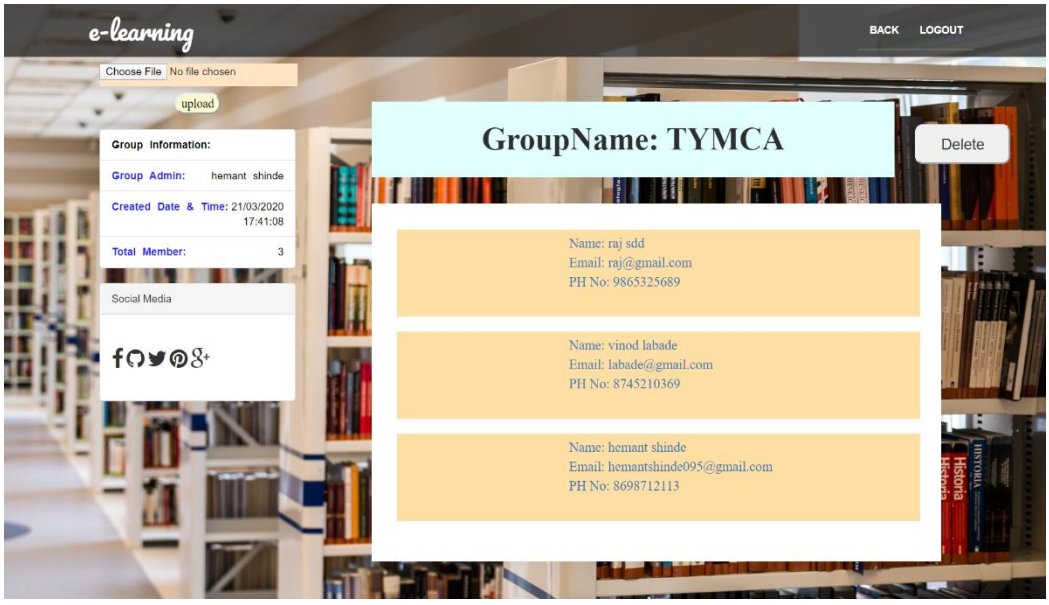


Fig 12: Group Information Page

This page can be accessed to gain information about various groups that is being created by teacher. It contains student's basic information which have joined that particular group along with group Admin and group creation date. Admin can also delete this particular group.

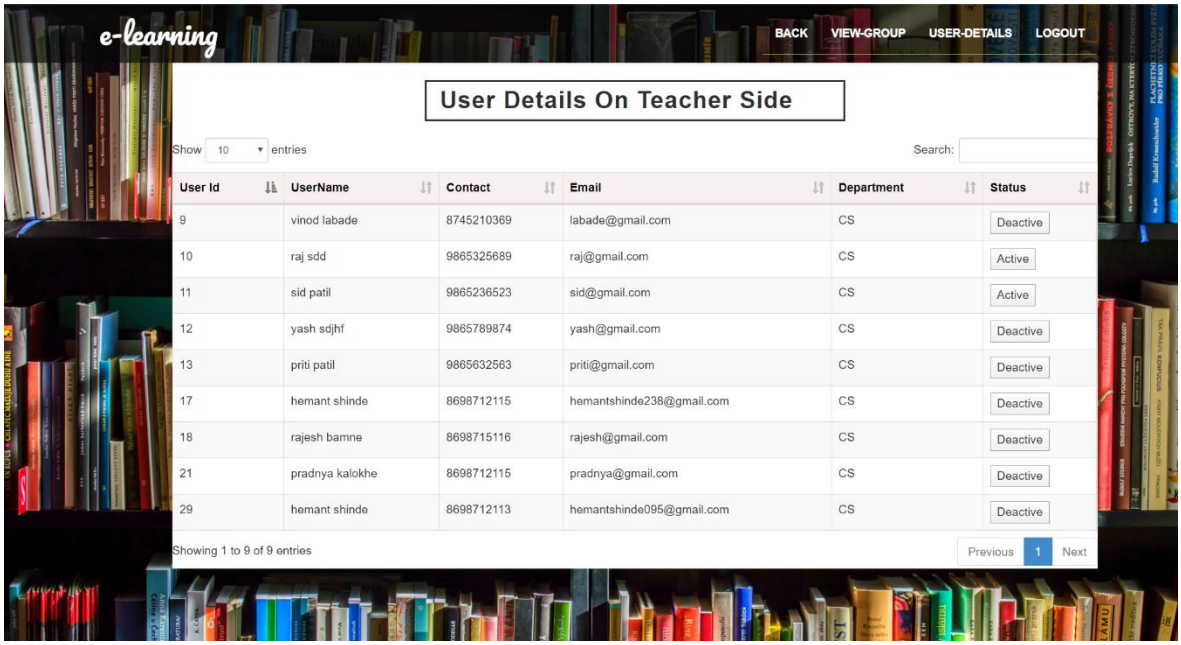


Fig 13: Student data

This page is accessed by teachers to gain the information of students of a particular group. Teachers can select which group of information they need.

CHAPTER 6

RESULTS AND EVALUATION

GUI Testing:
Graphical User Interface (GUIs) present interesting challenges for software engineers. Because of reusable components provided as part of GUI development environments, the creation of the user interface has become less time consuming and more precise. But, at the same time, the complexity of GUI has grown, leading to more difficulty in the design and execution of the test cases. Because many modern GUIs have the same look and same feel, a series of test cases can be derived.
Testcases:

General test cases of the system

Test Case ID	Test Scenario	Test Steps	Pre-requisite	Expected Result
TC_01	Verify the functionality of Registration form .	1- Navigate the URL .(AdminRegister.jsp) 2- Enter First name in text box. 3- Enter Last Name in text box. 4- Enter Valid Email address. 5- Enter Valid Password in text box 6- Enter password in text box of Confirm password	Register.jsp should be available	User should be able to enter the text in text box. Application should display the Valid message if you entered the incorrect email address . Application should display the message if password does not match
TC_02	Verify the functionality of Login 1- Email. 2- Password. 3- Login Button	1- Navigate the URL .(Login.jsp) 2- Enter Valid details in Email and Password . 3- Click on Login Button	login.jsp should be available	User should be able to entered the Valid Email address and Password. User should be Navigate to Next Page of Upload Image
TC_03	Verify the functionality of OTP verification	Register.jsp Fill the Details on Page Click on Add Activity Click on Submit Data button.		User should receive the OTP on registered email id and after entering OTP , application

				should allow user to login into the system
TC_04	Verify the functionality of Group creation and information about Group	Navigate to groupcreation.jsp Enter Group Name and Click on Submit button		User should be able to Create the Group.
TC_05	Verify the functionality of File Download	Navigate to filedownload.jsp Click on Download button		User should be able to download the file
TC_06	Verify the functionality of Exam	Navigate to exam.jsp Click on Start button		User should be able to start the exam, Exam result should be display

Security Test Cases and results

TC_01	Verify the Password entered by Login user	1- Navigate the Application and entered the Password	A password should be in encrypted format	Password should be in encrypted format and entered password should not display in the System
TC_02	Application or System should not allow invalid users	1- Navigate the Application and try to login into system by user not available in DB	Application or System should not allow invalid users	Application should not allow user to Login into System
TC_03	Verify the Check cookies and session time for application	1- Open the application in browser and verify the cookies 2- Remove the cookies of browser	Data of browser should not display	After removing Cookies and session , Data of browser should not display in Application

Performance Test Cases and results

TC-01	Verify response time is not more than 4 secs when multiple users access the website simultaneously	1- Open the application in multiple browser and verify the response	Response time should not be more than 4 sec	Response time should not be more than 4 sec when application

				has been opened in Multiple browser
TC-02	Verify response time of the Application Under Load is within an acceptable range when the network connectivity is slow	1- Open the application in Limited network speed and verify the response	Application should open properly	Application should open properly , if network speed is slow not exception should display
TC-03	Check database execution time when 500 records are read/written simultaneously.	1- Open the MYSQL and executed the Queries of Select all in Table	Proper Data should be display	Correct record should be fetch after entering Query.
TC-04	Verify response time of the application under low, normal, moderate and heavy load conditions.	1- Open the Application with different load condition	Application should open properly	Application should display correct Data with different Loads.

SOFTWARE VERIFICATION:

Evaluating the component to determine whether the product of given development phase satisfies the condition imposed at the start of the development.

- The buttons are in working conditions is checked (e.g. Home page).
- Walk through is performed with current modules.
- The errors are noted and corrected in verification.

SOFTWARE VALIDATION:

In this testing process, the evaluation of components are done by actually executing the code and checked whether the requirements are fulfilled or not.

- The validation is done by executing the code of developed

modules of user registration and login page, home screen, text plagiarism, code plagiarism, text and code plagiarism page.

- Black box and White box testing of modules are done.
- The technical errors are noted and corrected.

Analysis of algorithms:
Advanced Encryption Standard: Time required for encrypting the file is 2.63 secs.
Elliptical Curve Cryptography: Time required for generating the signature for each file is 3.72 secs.
K-Nearest Neighbor: Time required for classifying the dataset is 1.25secs

Chapter 7

Conclusion

We have tried in our system to provide new and innovative solution for media services that can be accessed from smart devices cloud based intelligent service environment with a fully integrated system, which will access files from the cloud and use it for their wellbeing. We have proposed the problem statement, the main moto of our system. We have proposed the system architecture of our system. A survey of previous systems has also been done through literature survey. Software development cycle has been depicted. The UML diagrams

such data flow, class, use case, sequence has been drawn. Testcases for various aspects have been generated. Analysis of system based on data retrieval from database, time required for performing security operations have been mentioned.

Chapter 6

References

List all the material used from various sources for making this project proposals

[1] Strahil A. Sokolov, Asen P.Zahariev, Stefan M. Vlaev , "Technology E-learning Evironment for Hybrid Cloud", International Symposium for Design and Technology in Electronic Packaging, vol. 3, pp. 38-42, 2017.

[2] Haibo Yi, Zhe Nie,"Implementation of Learning Management System Based on Cloud Computing", International Conference on Information Science and Control Engineering, vol. 2, pp. 478-481, 2017.

[3] Qasim Alajmi, Ali Sadiq "E-Learning Models: The Effectiveness of the Cloud Based E-Learning Model over the Traditional Elearning Model"4(3), pp. 311-316, 2017.

[4], Abiodun Kilanko, Falade Adesola and Isaac Odun-Ayo Member, "Elearning on Cloud-An Analysis",International MultiConference of Engineers and Computer Scientists vol. 49, pp. 399-404, 2019.

[5] M. A. H. Masud and X. Huang, "An e-learning system architecture based on cloud computing," system, vol. 10, 2017.

[6] Q. Alajmi and A. Sadiq, "in the preceding of Information Technology, Electronics and Mobile Communication Conference (IEMCON) IEEE 7th Annual,pp.1-5, 2016.

[7] C. Lee, Handbook of Research on Cloud-Based STEM Education for Improved Learning Outcomes. IGI Global, 2016.