Cryptography & Web Development

A Report Submitted

In Partial fulfillment of the requirement

For the degree of

Bachelor of Technology

Name	Roll Number
Kushagra Singh	201710101110009
Aman Mishra	201710101110014
Eram Bushra	201710101110029
Krishnam Rastogi	201710101110036

Guide: Er. Shoeb Ahmad

To the

FACULTY OF COMPUTER SCIENCE & ENGINEERING

Shri Ramswaroop Memorial University

TABLE OF CONTENTS

DECLARATION

We, Kushagra Singh (201710101110009), Aman Mishra (201710101110014), Eram Bushra (201710101110029) and Krishnam Rastogi (201710101110036) students of Bachelor of Technology, Computer Science & Engineering department at Shri Ramswaroop Memorial University, Lucknow hereby declare that the work presented in this project titled **"Cryptography And Web Development"** is outcome of our own work, is bona fide, correct to the best of our knowledge and this work has been carried out taking care engineering ethics.

We have completely taken care in acknowledging the contribution of others in this academic work. We further declare that in case of any violation of intellectual property rights or copyrights found at any stage, we as the candidates will be solely responsible for the same.

Date:

Place:

Signature:

Kusharga Singh

(201710101110036)

Aman Mishra

(201710101110014)

Eram Bushra

(201710101110029)

Krishnam Rastogi

(201710101110036)

ACKNOWLEDGEMENT

The present work will remain incomplete unless we express our feelings of gratitude towards a number of persons who delightfully co-operated with us in the process of this work.

First of all we would like to thank our Mentor for his encouragement and support during the course of my study. I extend my hearty and sincere gratitude to my project guide, ER. Shoeb Ahmad for his valuable direction, suggestions and exquisite guidance with ever enthusiastic encouragement ever since the commencement of this project.

This project would not have taken shape, without the guidance provided by project coordinators ER. Shoeb Ahmad who helped in our project and resolved all the technical as well as other problems related to the project and, for always providing us with a helping hand whenever we faced any bottlenecks, inspire of being quite busy with their hectic schedules.

Chapter 1: Introduction

1.1 Project Name

The **"Cryptography & Web Development"** has been developed to override the problems prevailing in the practicing manual system. This software is supported to eliminate and in some cases reduce the hardships faced by this existing system.

The application is reduced as much as possible to avoid errors while entering the data. It also provides error message while entering invalid data. No formal knowledge is needed for the user to use this system. Thus, by this all it proves it is user-friendly. E- Learning Management System, as described above, can lead to error free, secure, reliable and fast management system. It can assist the user to concentrate on their other activities rather to concentrate on the record keeping. Thus, it will help organization in better utilization of resources.

Every organization, whether big or small, has challenges to overcome and managing the information of Student, study material, syllabus, etc. This is designed to assist in strategic planning, and will help the organization is equipped with the right level of information and details for your future goals. Also, for those busy executive who are always on the go, our systems come with remote access features, which will allow you to manage your workforce anytime, at all times. These systems will ultimately allow you to better manage resources.

1.2 Preface

I. **Registration**: In this, first the interested students get registered by selecting their desired username and password and by providing the necessary details. Then each user profile will be maintained which can be edited by the user when desired. Each person will register only one time. Details of each person along with their username and password is saved permanently in the database in an encrypted format with the dynamic encryption algorithm used in this project.

II. **Login:** After providing the correct username and password, the user logs in to the LMS's Student portal. There the user can select the available subjects to further learn about them. If the user forgets his password, then he may get it reset by contacting the admin.

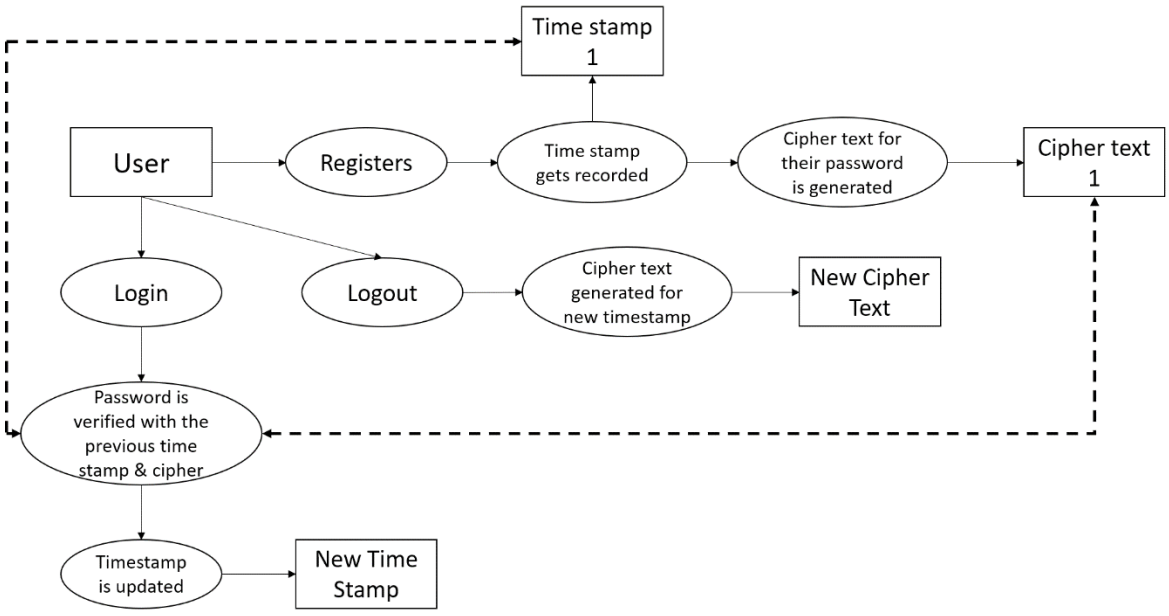
III. **Homepage:** After providing the correct credentials the user can login to their respective portals and access the actions accordingly. In the student homepage, the user can view different subjects and the respective topics and course content in it. In the admin panel, there are several actions that the admin can perform and in the teacher panel, the teacher can view and add different subjects and their respective topics.

1.3 About the Dynamic Encryption Algorithm

The algorithm used in this system to encrypt the user's passwords efficiently and in a safe manner is developed by Krishnam Rastogi. The algorithm is dynamic in nature and it works on the principle of timestamping. This algorithm enables the encryption key and the cipher text at every login and logout of the user and the encryption key and the cipher text gets initialized at the time of the registration of the user. If the user had not logged out of the previous session then, they might get locked out of their account and would have to contact the admin for getting their password reset.

The user can only login their account at one device at a time and this feature actually increases the security. The use case of this feature would be very beneficial in financial organizations where any financial account should only be accessed one at a time. Another use case would be in this project as well, as if the organization using it sells their courses on this LMS then it could avoid the users who share their passwords with other students to use and access it at multiple places at same time.

Flow chart of the algorithm



1.4 Definition of Project Technology

1.4.1 HTML:

I. HTML is the standard markup language for documents designed to be displayed in a web browser.
II. It can be assisted by technologies such as Cascading Style Sheets (CSS) and scripting languages such as JavaScript.
III. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages.

1.4.2 CSS:

I. Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language such as HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript.
II. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts.
III. Separation of formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods
IV. CSS also has rules for alternate formatting if the content is accessed on a mobile device.

1.4.3 PHP:

I. PHP is a general-purpose scripting language especially suited to web development. It stands for the recursive initialism PHP: Hypertext Preprocessor.
II. PHP code is usually processed on a web server by a PHP interpreter implemented as a module, a daemon or as a Common Gateway Interface (CGI) executable.
III. The standard PHP interpreter, powered by the Zend Engine, is free software released under the PHP License. PHP has been widely ported and can be deployed on most web servers on almost every operating system and platform, free of charge.

1.4.4 JavaScript:

I. JavaScript, often abbreviated as JS, is a scripting language that conforms to the ECMAScript specification.
II. JavaScript is high-level, often just-in-time compiled, and multi-paradigm. It has curly-bracket syntax, dynamic typing, prototype-based object-orientation, and first-class functions.
III. JavaScript enables interactive web pages and is an essential part of web applications. The vast majority of websites use it for client-side page behavior, and all major web browsers have a dedicated JavaScript engine to execute it.
IV. As a multi-paradigm language, JavaScript supports event-driven, functional, and imperative programming styles.

1.4.5 MySQL:

I. MySQL Database Service is a fully managed database service to deploy cloud-native applications.
II. Native, real-time analytics
III. Eliminate the cost, complexity, and risk of ETL
IV. Protect your databases against data breaches
V. Meet industry and regulatory compliance

Chapter 2: Requirement analysis and Feasibility study

2.1 Requirement Analysis

2.1.1 Information Gathering

The proposed system has the following requirements:

I. System needs store information about new entry of topics and their respective contents.
II. System needs to help the admin to keep information of Student and the subjects and view and make changes to them.
III. System needs to keep the record of TEACHER and STUDENT and ADMIN
IV. System needs to update and delete the record.
V. System also needs a search area.
VI. It also needs a security system and encryption to prevent data breach.

2.1.2 Hardware Requirements

Hardware	**Minimum Requirements**
Computer/Laptop	4Ghz Multicore processor
Memory (RAM)	At least 4GB preferably higher
Hard disk space	At least 5 GBs

2.1.3 Software Requirements

Software	**Minimum Requirements**
Operating System	MS Windows, Linux or Mac OS x
Editor	Sublime text, VS Code, Notepad++, GEdit, Vim, etc.

2.1.4 Usability Requirements

Any internet browser which supports JavaScript will work fine, eg: Mozilla Firefox, Google Chrome, Microsoft Edge, Safari

2.1.5 Security Requirements

a. The following basic security aspects should be met for e-learning platforms: authenticity, access control, confidentiality, integrity, availability, non-repudiation.
b. A secure authentication is required to identify the user who will use the web application and to determine his access privileges. This mechanism prevents the attackers to access another user's account, to view sensitive information or to perform unauthorized operations.
c. The access control is realized during the authentication time when the user is granted with all the necessary rights. In this way the user will perform in the system only his allowed operations. The role-based authorization model is an approach of restricting the system access of unauthorized users; it allows groups definition, users inclusion in groups or even groups in another groups.
d. It uses the dynamic encryption algorithm which changes the encryption key and the cipher text in the database after every login and logout of the user and even if someone gets to have the database at an instance, the passwords of the user will be secure when the user either logs in or logs out of their account.

2.2 Feasibility Study

2.2.1 Technical Feasibility

Technical feasibility evaluates the technical complexity of the expert system and often involves determining whether the expert system can be implemented with state-of-the-art techniques and tools. In the case of expert systems, an important aspect of technical feasibility is determining the shell in which the system will be developed. The shell used to develop an expert system can be an important determinant to its quality and makes it vital to the system's success. Although the desirable characteristics of an expert system shell will depend on the task and domain requirements, the shell must be flexible enough to build expert reasoning into the system effectively. It must also be easily integrated with existing computer-based systems. Furthermore, a shell providing a user-friendly interface encourages end users to use the system more frequently.

2.2.2 Operational Feasibility

Operational feasibility is dependent on human resources available for the project and involves projecting whether the system will be used if it is developed and implemented.
Operational feasibility is a 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. Operational feasibility reviews the willingness of the organization to support the proposed system. This is probably the most difficult of the feasibilities to gauge. In order to determine this feasibility, it is important to understand the management commitment to the proposed project. If the request was initiated by management, it is likely that there is management support and the system will be accepted and used. However, it is also important that the employee base will be accepting of the change.

2.2.3 Economical Feasibility

Once the technical feasibility and market studies are complete, it is time to determine Business Feasibility. The first purpose of this effort is to financially model the venture opportunity and achieve a break-even analysis. In other words, based upon the costs of goods sold, capital costs, and management and administration, how much revenue generated from units sold is required to break-even and over what period of time.

Once a break-even analysis is developed, the entrepreneurs can develop realistic financial projections for best case and worst-case scenarios. These scenarios will be critical in strategic planning, milestone development and venture valuation analysis. The simple objective is to determine what level of revenue is required to satisfy the return on investment demanded by the founder and/or the investors. The economic feasibility step of business development is that period during which a break-even financial model of the business venture is developed based on all costs associated with taking the product from idea to market and achieving sales sufficient to satisfy debt or investment requirements

Chapter 3: System Analysis & Design

3.1 System Analysis

In this phase, a logical system is built which fulfils the given requirements. Design phase of software development deals with transforming the client's requirements into a logically working system. Normally, design is performed in the following in the following two steps:

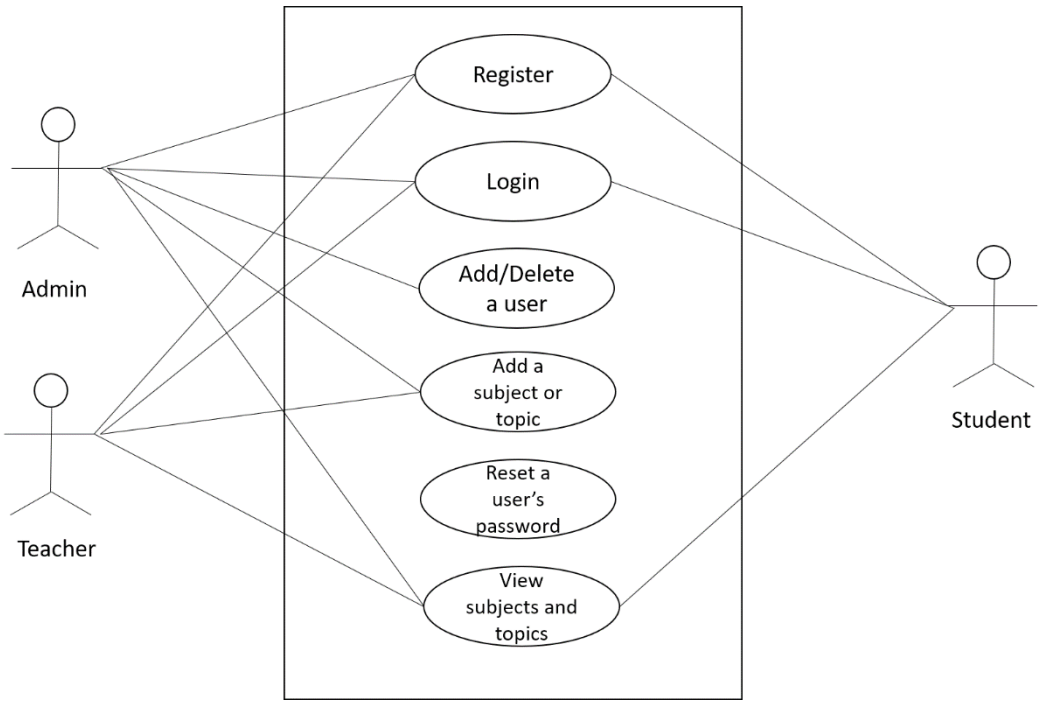
I. **Primary Design Phase:** -In this phase, the system is designed at block level. The blocks are created on the basis of analysis done in the problem identification phase. Different blocks are created for different functions emphasis is put on minimizing the information flow between blocks. Thus, all activities which require more interaction are kept in one block.
II. **Secondary Design Phase**: In the secondary phase the detailed design of every block is performed.

3.2 System Design

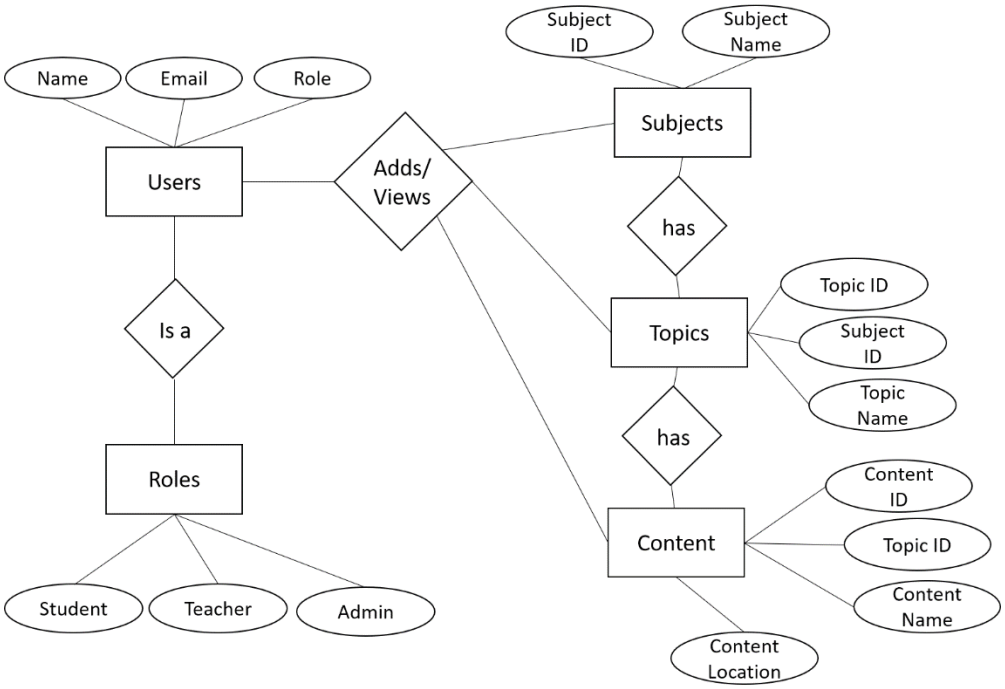
General task involved in the design process are following:

a) Design various blocks for overall system processes.
b) Design smaller, compact and workable modules in each block.
c) Design various database structures.
d) Specify details of programs to achieve desired functionality.
e) Design the form of inputs, and outputs of the system.
f) Perform documentation of the design.
g) System reviews.

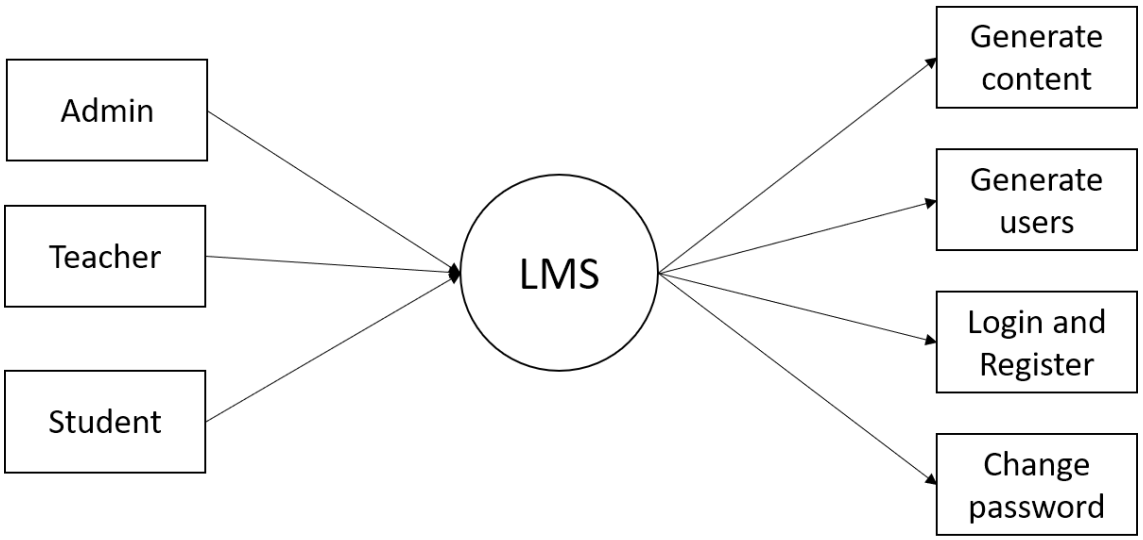
3.2.1 Use Case Diagram



3.2.2 ER Diagram

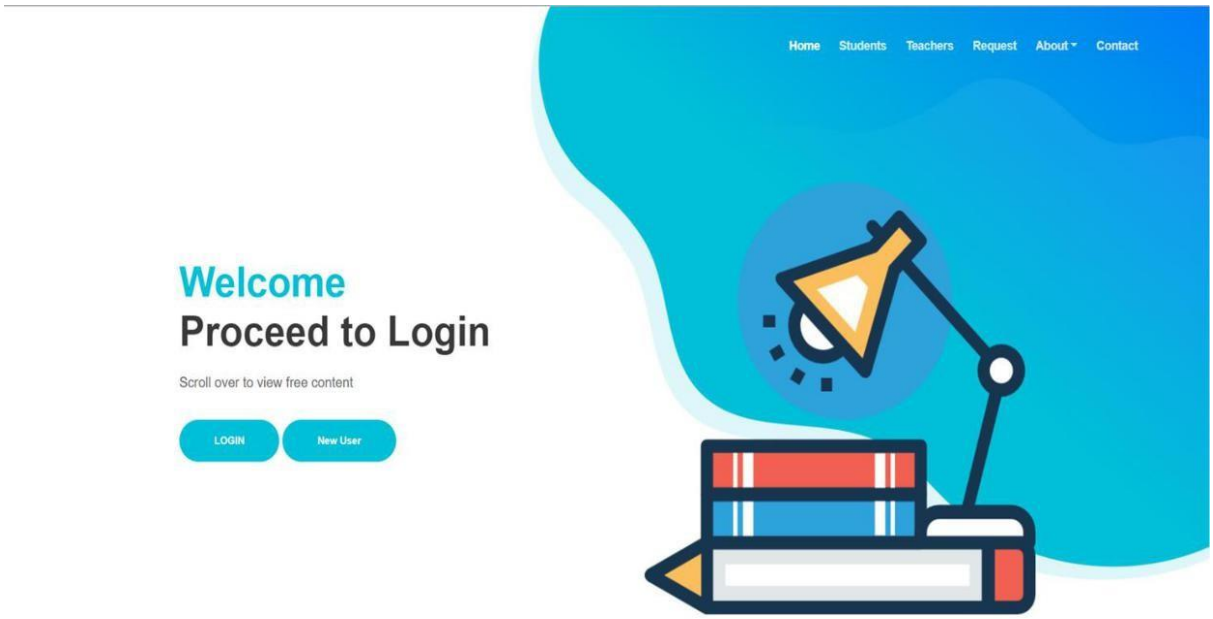


3.2.3 Data Flow Diagram

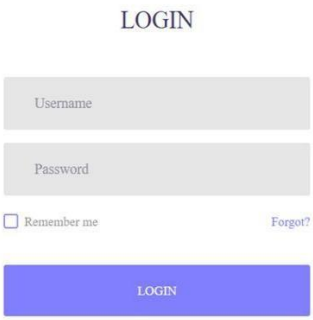


3.2.3 Snapshots

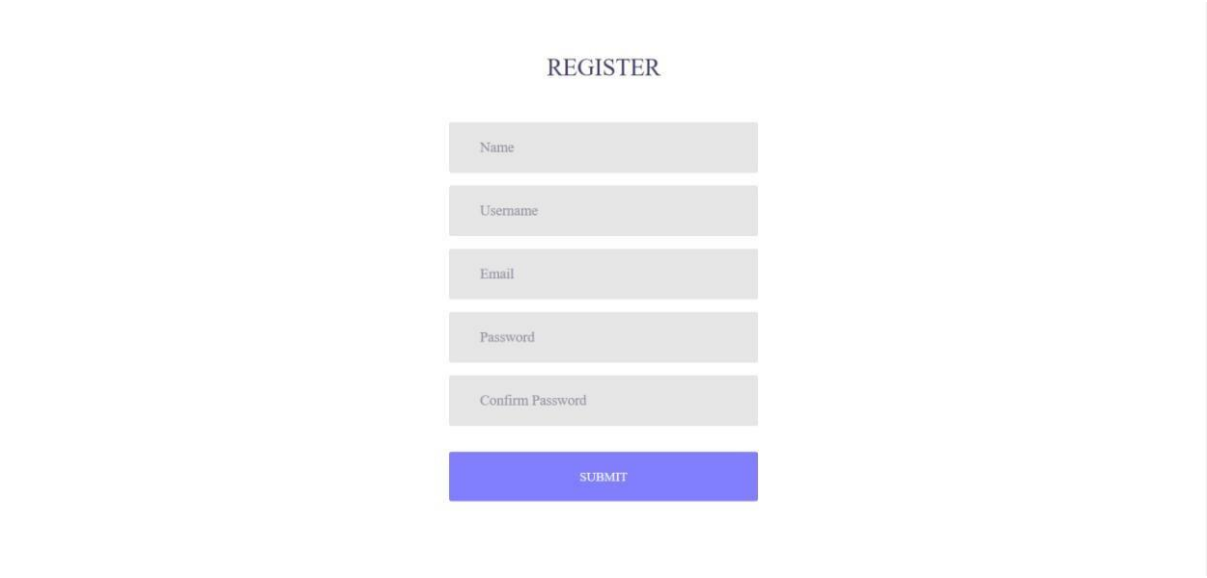
Landing Page



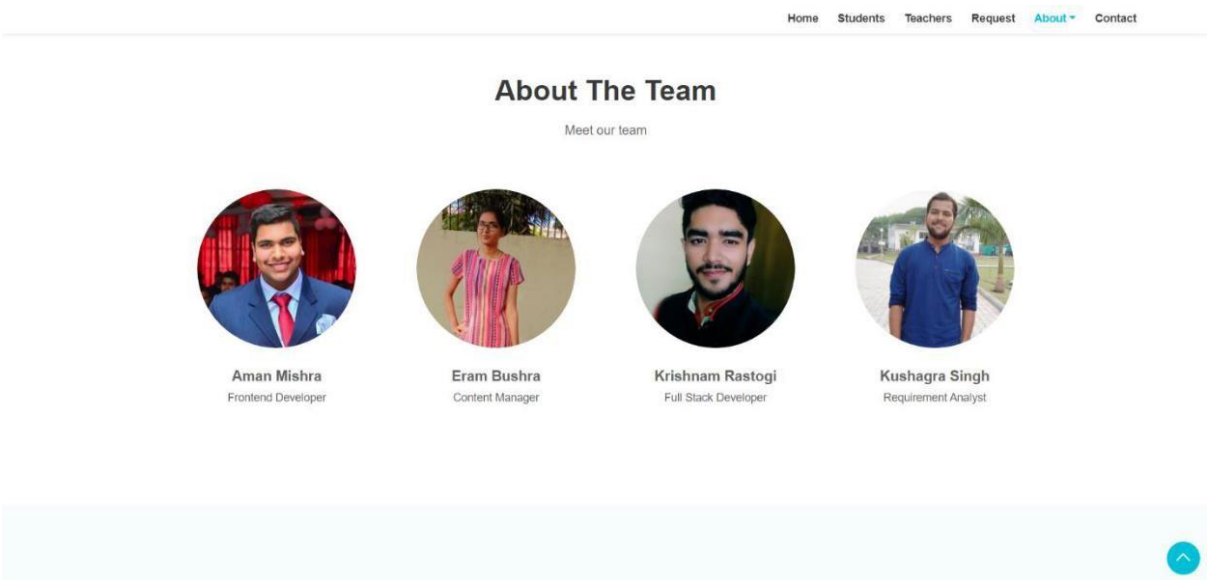
Login page



Registration Page



Team Members



Chapter 4: Testing

4.1 About the technologies used

i) HTML: HTML stands for Hyper Text Markup Language, which is the most widely used language on Web to develop web pages. HTML was created by Berners-Lee in late 1991 but "HTML 2.0" was the first standard HTML specification which was published in 1995. HTML 4.01 was a major version of HTML and it was published in late 1999. Though HTML 4.01 version is widely used but currently we are having HTML-5 version which is an extension to HTML 4.01, and this version was published in 2012.

Why to Learn HTML?

- Originally, HTML was developed with the intent of defining the structure of documents like headings, paragraphs, lists, and so forth to facilitate the sharing of scientific information between researchers. Now, HTML is being widely used to format web pages with the help of different tags available in HTML language.
- HTML is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning HTML:
    - Create Web site - You can create a website or customize an existing web template if you know HTML well.
    - Become a web designer - If you want to start a carrer as a professional web designer, HTML and CSS designing is a must skill.
    - Understand web - If you want to optimize your website, to boost its speed and performance, it is good to know HTML to yield best results.
    - Learn other languages - Once you understands the basic of HTML then other related technologies like javascript, php, or angular are become easier to understand.

ii) CSS: CSS is used to control the style of a web document in a simple and easy way.CSS is the acronym for **"Cascading Style Sheet"**.

Why to Learn CSS?

- Cascading Style Sheets, fondly referred to as CSS, is a simple design language intended to simplify the process of making web pages presentable.
- CSS is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning CSS:
    - Create Stunning Web site - CSS handles the look and feel part of a web page. Using CSS, you can control the color of the text, the style of fonts, the spacing between paragraphs, how columns are sized and laid out, what background images or colors are used, layout designs,variations in display for different devices and screen sizes as well as a variety of other effects.
    - Become a web designer - If you want to start a carrer as a professional web designer, HTML and CSS designing is a must skill.
    - Control web - CSS is easy to learn and understand but it provides powerful control over the presentation of an HTML document. Most commonly, CSS is combined with the markup languages HTML orXHTML.
    - Learn other languages - Once you understands the basic of HTML and CSS then other related technologies like javascript, php, or angular are become easier to understand.

iii) PHP: The PHP Hypertext Preprocessor (PHP) is a programming language that allows web developers to create dynamic content that interacts with databases. PHP is basically used for developing web-based software applications. This tutorial helps you to build your base with PHP.

Why to Learn PHP?

- PHP started out as a small open source project that evolved as more and more people found out how useful it was. Rasmus Lerdorf unleashed the first version of PHP way back in 1994.
- PHP is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning PHP.
    - PHP is a recursive acronym for "PHP: Hypertext Preprocessor".
    - PHP is a server side scripting language that is embedded in HTML. It is used to manage dynamic content, databases, session tracking, even build entire e-commerce sites.
    - It is integrated with a number of popular databases, including MySQL, PostgreSQL, Oracle, Sybase, Informix, and Microsoft SQL Server.
    - PHP is pleasingly zippy in its execution, especially when compiled as an Apache module on the Unix side. The MySQL server, once started, executes even very complex queries with huge result sets in record-setting time.
    - PHP supports a large number of major protocols such as POP3, IMAP, and LDAP. PHP4 added support for Java and distributed object architectures (COM and CORBA), making n-tier development a possibility for the first time.
    - PHP is forgiving: PHP language tries to be as forgiving as possible.
    - PHP Syntax is C-Like.

iv) JavaScript: JavaScript is a lightweight, interpreted programming language. It is designed for creating network-centric applications. It is complimentary to and integrated with Java. JavaScript is very easy to implement because it is integrated with HTML. It is open and cross-platform.

Why to Learn JavaScript?

Javascript is a MUST for students and working professionals to become a great Software Engineer specially when they are working in Web Development Domain. I will list down some of the key advantages of learning Javascript:

- Javascript is the most popular programming language in the world and that makes it a programmer's great choice. Once you learnt Javascript, it helps you developing great front-end as well as back-end softwares using different Javascript based frameworks like jQuery, Node.JS etc.
- Javascript is everywhere, it comes installed on every modern web browser and so to learn Javascript you really do not need any special environment setup. For example Chrome, Mozilla Firefox , Safari and every browser you know as of today, supports Javascript.
- Javascript helps you create really beautiful and crazy fast websites. You can develop your website with a console like look and feel and give your users the best Graphical User Experience.
- JavaScript usage has now extended to mobile app development, desktop app development, and game development. This opens many opportunities for you as Javascript Programmer.
- Due to high demand, there is tons of job growth and high pay for those who know JavaScript. You can navigate over to different job sites to see what having JavaScript skills looks like in the job market.
- Great thing about Javascript is that you will find tons of frameworks and Libraries already developed which can be used directly in your software development to reduce your time to market.

v) MySQL:- MySQL is the most popular Open Source Relational SQL Database Management System. MySQL is one of the best RDBMS being used for developing various web-based software applications. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. This tutorial will give you a quick start to MySQL and make you comfortable with MySQL programming.

What is a Database?

A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating the data it holds.

Other kinds of data stores can also be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those type of systems.

Nowadays, we use relational database management systems (RDBMS) to store and manage huge volume of data. This is called relational database because all the data is stored into different tables and relations are established using primary keys or other keys known as Foreign Keys.

A Relational DataBase Management System (RDBMS) is a software that −

- Enables you to implement a database with tables, columns and indexes.
- Guarantees the Referential Integrity between rows of various tables.
- Updates the indexes automatically.
- Interprets an SQL query and combines information from various tables.

4.2 Testing

Testing is the process of executing a program with the aim of finding errors. To make our software perform well it should be error-free. If testing is done successfully it will remove all the errors from the software.

Principles of Testing:

I. All the test should meet the customer requirements
II. To make our software testing should be performed by a third party
III. Exhaustive testing is not possible. As we need the optimal amount of testing based on the risk assessment of the application.
IV. All the test to be conducted should be planned before implementing it
V. It follows the Pareto rule(80/20 rule) which states that 80% of errors come from 20% of program components.
VI. Start testing with small parts and extend it to large parts.

Types of Testing:

1) Unit Testing
2) Integration Testing
3) System Testing

4.2.1 UNIT TESTING

a. Functionality of the entire module/forms.
b. Validations for user input.
c. Checking of the Coding standards to be maintained during coding.
d. Testing the module with all the possible test data.
e. Testing of the functionality involving all type of calculations etc.
f. Commenting standard in the source files.

After completing the Unit testing of all the modules, the whole system is integrated with all its dependencies in that module. While System Integration, We integrated the modules one by one and tested the system at each step. This helped in reduction of errors at the time of the system testing.

4.2.2 INTEGRATION TESTING

Integration Testing is a level of software testing where individual units are combined and tested to verify if they are working as they intend to when integrated. The main aim here is to test the interface between the modules.

Just unit testing is not enough for multiple reasons like:

- A module/unit is usually designed by an individual software developer whose techniques and programming logic differs from that of other programmers.
- Often at the time of module development, user requirements change and these new requirements may not be unit tested. This instigates issues.
- Issues like data formatting, error trapping, hardware interfaces, and third-party service interfaces are sometimes missed during unit testing.

4.2.3 SYSTEM TESTING

a. Functionality of the entire system as a whole.
b. User Interface of the system.
c. Testing the dependent modules together with all the possible test data scripts.
d. Verification and Validation testing.
e. Testing the reports with all its functionality.

Chapter 5: Advantages and Limitations of the developed system

5.1 Advantages of developed system

I. The encryption algorithm allows the student to only login at one device at a time and this is advantageous for the organization if they are selling any course as the student couldn’t share their passwords with their friends.
II. You are able to link the various resources in several varying formats.
III. It is a very efficient way of delivering courses online.
IV. Due to its convenience and flexibility, the resources are available from anywhere and at any time.
V. Everyone, who are part time students or are working full time, can take advantage of web-based learning.
VI. Web-based learning promotes active and independent learning.
VII. As you have access to the net 24x7, you can train yourself anytime and from anywhere also.
VIII. It is a very convenient and flexible option; above all, you don't have to depend on anyone for anything.
IX. Not only can you train yourself on a day-to-day basis, but also on weekends or whenever you have the free time to. There is no hard and fast rule.
X. The video instructions that are provided for audio and video learning can be rewound and seen and heard again and again if you do not happen to understand the topic first time around.

5.2 Limitations of developed system

I. The encryption algorithm used in this project to encrypt the username and password only works for the text data and do not work for the multimedia files and documents
II. The user always have to logout of their account otherwise they would get locked out of their account and then have to contact the admin to get their password reset.
III. Currently due to lack of proper investment the study content is only limited to video lectures and pdf documents and the video lectures are to be hosted on YouTube.
IV. Online student feedback is limited
V. E-Learning can cause social Isolation
VI. E-Learning requires strong self-motivation and time management skills
VII. Lack of communicational skill development in online students
VIII. Online instructors tend to focus on theory rather than practice

Chapter 6: Conclusion and Suggestions for further work

6.1 Conclusion

Our project is only a humble venture to satisfy the needs to manage their project work. Several user friendly coding have also adopted. This package shall prove to be a powerful package in satisfying all the requirements of the school. The objective of software planning is to provide a frame work that enables the manger to make reasonable estimates made within a limited time frame at the beginning of the software project and should be updated regularly as the project progresses.

At the end it is concluded that we have made effort on following points:

a) A description of the background and context of the project and its relation to work already done in the area.
b) Made statement of the aims and objectives of the project.
c) The description of Purpose, Scope, and applicability.
d) We &fine the problem on which we are working in the project.
e) We describe the requirement Specifications of the system and the actions that can be done on these things.
f) We understand the problem domain and produce a model of the system, which describes operations that can be performed on the system.
g) We included features and operations in detail, including screen layouts.
h) We designed user interface and security issues related to system.
i) Finally the system is implemented and tested according to test cases.

6.2 Suggestion for Further Work

In a nutshell, it can be summarized that the future scope of the project circles around maintaining information regarding:

- We can add printer in future.
- We can give more advance software for E-learning Management System including more facilities
- We will host the platform on online servers to make it accessible worldwide
- Integrate multiple load balancers to distribute the loads of the system
- Create the master and slave database structure to reduce the overload of the database queries
- Implement the backup mechanism for taking backup of codebase and database on regular basis on different servers
- The above mentioned points are the enhancements which can be done to increase the applicability and usage of this project. Here we can maintain the records of Assignment and Student. Also, as it can be seen that now-a-days the players are versatile, i.e. so there is a scope for introducing a method to maintain the E-learning Management System.
- Enhancements can be done to maintain all the Assignment, Student, TEACHER, QUIZ, QUESTION.

We have left all the options open so that if there is any other future requirement in the system by the user for the enhancement of the system then it is possible to implement them. ln the last we would like to thanks all the persons involved in the development of the system directly or indirectly. We hope that the project will serve its purpose for which it is develop there by underlining success of process.

Chapter 7: References

- https://www.w3schools.com/
- https://en.wikipedia.org/
- https://www.php.net/
- https://www.mysql.com/
- https://css-tricks.com/
- https://www.javascript.com/
- https://www.python.org/
- https://www.youtube.com/
- https://www.apachefriends.org/