****

**An**

**Internship Assessment Report**

On

**User Authentication**

At

**CETPA Infotech Private Limited**

**Report submitted in partial fulfillment of the requirement for award of**

**Bachelor of Technology**

**Name of student: Prince Supervisor Name: Mr Aditya Batra**

**Roll No: 2201430109011 Designation: Assistant Professor**

**Section: CSE3**

**Department of Computer Science and Engineering**

**IMS ENGINEERING COLLEGE**

**NH-09, Adhyatmik Nagar, Ghaziabad-201015**

**(2024-25)**

**Vision and Mission of the Institute and Department**

**Vision of the Institute**

To make IMSEC an Institution of Excellence for empowering students through technical education coupled with incorporating values and developing engineering acumen for innovations and leadership skills for the betterment of society.

**Mission of the Institute**

**Mission 1**: To promote academic excellence by continuous learning in core and emerging Engineering areas using innovative teaching and learning methodologies.

**Mission 2**: To inculcate values and ethics among the learners.

**Mission 3**: To promote industry interactions and produce young entrepreneurs.

**Mission 4**: To create a conducive learning and research environment for life-long learning to develop the students as technology leaders and entrepreneurs for addressing societal needs.

**Vision of the Department**

To provide globally competent professionals in the field of Computer Science & Engineering embedded with sound technical knowledge, aptitude for research and innovation with ethical values to cater to the industrial & societal needs.

**Mission of the Department**

M1:To provide quality undergraduate education in both the theoretical & applied foundations of Computer Science Engineering.

M2: Conduct research to advance the state of the art in Computer Science & Engineering and integrate the research results as innovations.

M3: To inculcate team building skills and promote life-long learning with a high societal and ethical values.

**Program Outcomes (POs)**

|  |  |
| --- | --- |
| **S. No.** | **Program Outcomes / Program Specific Outcomes** |
| **PO1.** | **Engineering knowledge**: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems. |
| **PO2.** | **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences. |
| **PO3.** | **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations. |
| **PO4.** | **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions. |
| **PO5.** | **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations. |
| **PO6.** | **The engineer and society:** apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice. |
| **PO7.** | **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development. |
| **PO8.** | **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice. |
| **PO9.** | **Individual and team work**: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings. |
| **PO10.** | **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions. |
| **PO11.** | **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments. |
| **PO12.** | **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change. |

**Program Specific Outcomes (PSOs)**

#### PSO1: To analyze and demonstrate, the recent engineering practices, ethical values and strategies in real time world problems to meet the challenges for the future.

**PSO2**: To develop adaptive computing system using computational intelligence strategies and algorithmic design to address diverse challenges in data analysis and machine learning.

**Program Educational Objectives (PEOs)**

**PEO1**: Possess core theoretical and practical knowledge in Computer Science and Engineering for successful career development in industry, pursuing higher studies or entrepreneurship

**PEO2**: Ability to imbibe life-long learning for global challenges to impact society and environment.

**PEO3**: To demonstrate work productivity with leadership and managerial skills having ethics and human value in progressive career path.

**PEO4**: To exhibit communication skill and collaborative skill plan and participate in multidisciplinary fields of Computer Science & Engineering.

**CO-PO-PSO MAPPNG FOR ACADEMIC SESSION 2023-24**

**Course Name:** Internship Assessment **AKTU Course Code**: KCS752

**Semester/Year**: VII/ 4th **NBA Code**: C406

**Course Coordinator**: Basudeo Singh Roohani

**Course Outcomes**

|  |  |  |
| --- | --- | --- |
| **CO. No.** | **DESCRIPTION** | **COGNITIVE LEVEL (BLOOMS TAXONOMY)** |
| **CO1(C406.1)** | Developing a technical artifact requiring new technical skills and effectively utilizing a new software tool to complete a task | **K4,K5** |
| **CO2(C406.2)** | Writing requirements documentation, Selecting appropriate technologies, identifying and creating appropriate test cases for systems. | **K5,K6** |
| **CO3(C406.3)** | Demonstrating understanding of professional customs & practices and working with professional standards. | **K4,K5** |
| **CO4(C406.4)** | Improving problem-solving, critical thinking skills and report writing. | **K4,K5** |
| **CO5(C406.5)** | Learning professional skills like exercising leadership, behaving professionally, behaving ethically, listening effectively, participating as a member of a team, developing appropriate workplace attitudes | **K2,K4** |

**CO-PO-PSO Mapping**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **PO1** | **PO2** | **PO3** | **PO4** | **PO5** | **PO6** | **PO7** | **PO8** | **PO9** | **PO 10** | **PO 11** | **PO 12** | **PSO1** | **PSO2** |
| **C406.1** | 3 | 3 | 3 | 3 | 3 | 2 | 1 | 2 | 2 | 2 | 2 | 3 | 3 | 3 |
| **C406.2** | 3 | 3 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 3 | 1 | 1 | 2 | 3 |
| **C406.3** | 1 | 1 | 1 | 1 | 1 | 3 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 1 |
| **C406.4** | 3 | 3 | 3 | 3 | 3 | 2 | 1 | 1 | 2 | 3 | 1 | 3 | 1 | 1 |
| **C406.5** | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 3 | 3 | 3 | 3 | 1 | 1 | 1 |
| **C406** | **2.2** | **2.2** | **2** | **2** | **2** | **2** | **1.4** | **2.2** | **2.2** | **2.6** | **1.8** | **2** | **1.8** | **1.8** |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **S.No** | **Content** | **Page No** |
| 1. | Internship Certificate | 1 |
| 2. | Declaration | 2 |
| 3. | Acknowledgement | 3 |
| 4. | List of Figures | 4 |
| 5. | List of Tables | 5 |
| 6. | Introduction to the Industry/Institution | 6 |
| 7. | **Company Profile:**   1. Company name with full address 2. Establishment Year, Owner Name, Annual Turnover etc. 3. Name of business of the Industry/Institute (Training Institute/Software Company etc.) 4. Add organizational Chart | 7 |
| 8. | Activities of the Company |  |
| 9. | Summer internship at a Glance(brief introduction) |  |
| 10. | Major Customers/Competitors |  |
| 11. | **CHAPTER 1: INTRODUCTION**   1. Background 2. Objectives 3. Scope of Project 4. Conclusion |  |
| 12. | **CHAPTER 2: METHODOLOGY**   1. Problem Definition 2. Literature Survey 3. Tools and Technology used |  |
| 13. | **CHAPTER 3: SYSTEM DESIGN**   1. Basic Modules 2. Data Flow Diagram 3. User interface design 4. Security Issues |  |
| 14. | **CHAPTER 4: IMPLEMENTATION AND TESTING**   1. Coding 2. Testing |  |
| 15. | **CHAPTER 5: RESULTS AND DISCUSSION**   1. Test Reports |  |
| 16. | **CHAPTER 6: CONCLUSIONS**   1. Limitations of the System 2. Future Scope of the Project 3. References |  |

**Company Letterhead**

[Date]

**Certificate of Completion**

This is to certify that Mr. Prince, Roll No. 2201430109011 bonafide student of IMS Engineering College, Ghaziabad, U.P has successfully completed the Offline Summer Internship on MERN Full Stack Web Development Program at CETPA Infotech Private Limited. The program took place from 05-06-2024 to 03-07-2024, with duration of four weeks. During this period, Mr. Prince has worked on a project “**User Authentication**” demonstrating exceptional enthusiasm, professionalism, and a strong work ethic.

We believe that Mr. Prince has gained valuable practical experience and has made a significant contribution to our company/organization during his time with us. We hope that this internship has provided Mr. Prince with a strong foundation for their future career endeavors.

We wish him continued success in his academic pursuits and professional journey.

Sincerely,

(Raj Kumar)

(Designation)

(Company Name)

(Company Address with Pin Code)

(Contact Number)

(Email Address)

## DECLARATION

*I hereby declare that the work, which is being presented in this report” User Authentication” in partial fulfillment of the requirement for the award of Bachelor of Technology in Computer Science & Engineering and submitted to the Department of the Computer Science & Engineering, IMS Engineering College, Ghaziabad, is an authentic record of my work carried within the premises of “ CETPA Infotech Private Limited”, under the supervision of Dr. Aditya Batra (Assistent Professor).*

*The contents of this report, in full or parts have not been submitted to any other Institute or University for the award of any other degree or diploma and are free from plagiarism.*

### Signature of the student

**Name** *:*

**Roll No***:*

**Section:**

**Date:**

## ACKNOWLEDGEMENT

I am extremely grateful to “CETPA Infotech Private Limited” for providing me the opportunity to carry out my Summer Internship at their facility. Special thanks are due to (Name of Manager/Engineer/ Supervisor with designation) for their continuous support and guidance in being my mentor. Last but not least, I would like to extend my gratefulness to all the supervisors and technicians, right from the highest to simplest, for their constant and enthusiastic support.

My Sincere thanks to respected Director Prof. (Dr.) Vikram Bali, Head of the Department Prof.(Dr.) Sonali Mathur, Co-ordinators Internship Assessment Mr. Basudeo Singh Roohani. Ms. Shanu Priya Chauhan and all the faculty members for providing me wonderful support and guidance.

### Signature of the student

**Name** :

**Roll No**

**Section:**

**COMPANY PROFILE**

**a) Company name with full address**

CETPA Infotech Pvt. Ltd. is a well-known training and development company in India, specializing in IT and software development training. Established in 2002.Its registered office is in Noida-201301, Uttar Pradesh.

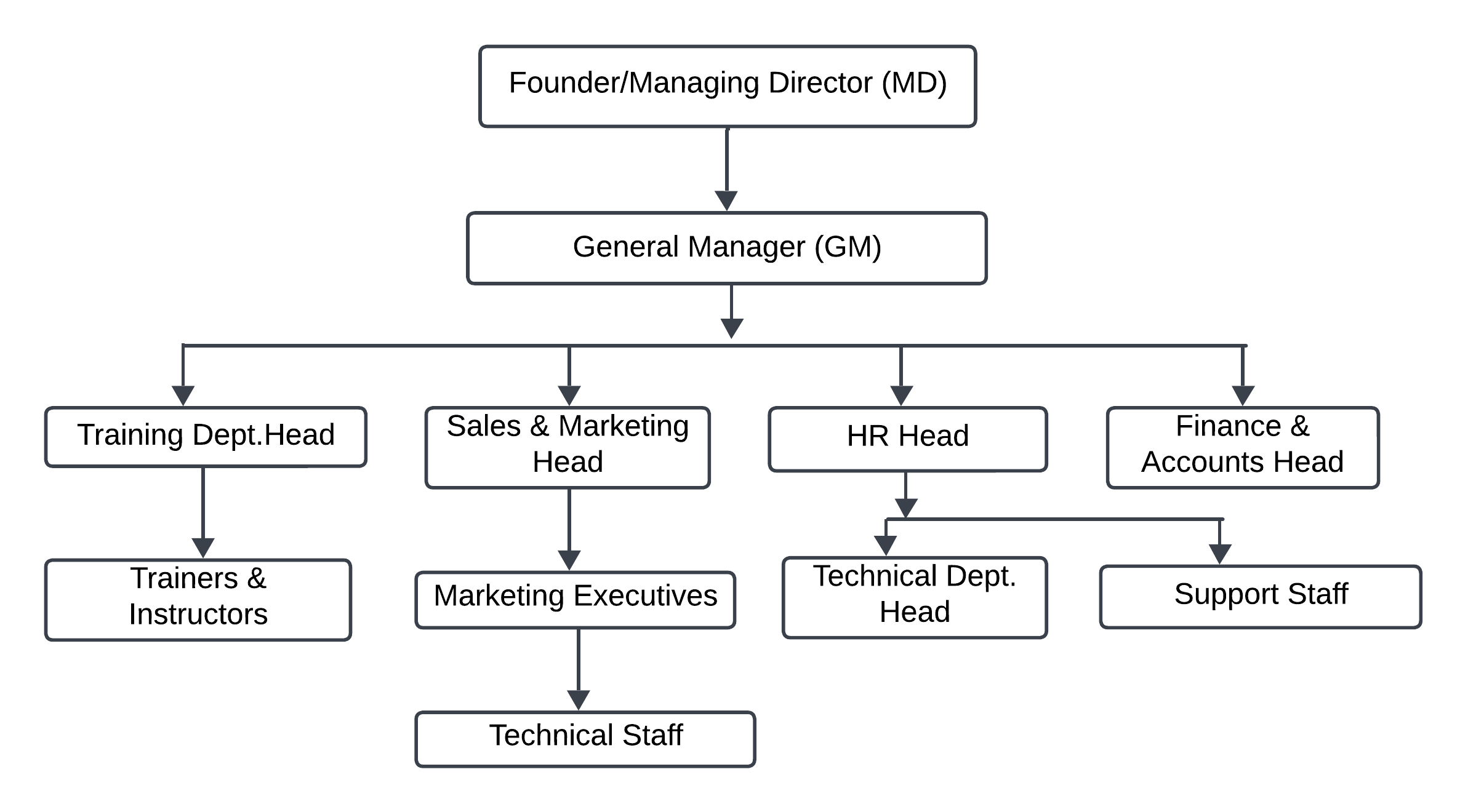
**b) Establishment Year, Owner Name, Annual Turnover etc.**

CETPA Infotech Pvt. Ltd., established in 2002, is a leading IT training and development company in India. Founded by Mr. Vishvajit Srivastava, who also serves as the Managing Director, CETPA has its headquarters in Noida, Uttar Pradesh, with additional branches in cities like Lucknow, Roorkee, and Dehradun. The company specializes in providing industry-relevant training programs, including certifications in programming, web development, data science, and cutting-edge technologies like AI and IoT. While specific details about its annual turnover are not publicly disclosed, the company's consistent reputation and wide reach in the IT education sector highlight its significant presence and influence in the industry.

**c) Name of business of the Industry/Institute /Software Company etc.)**

CETPA Infotech Private Limited is a global skills and talent development company that offers a wide range of learning and training solutions for individual, working professional, institutions and government entities.

**d) Organizational Chart**

****

**ACTIVITES OF THE COMPANY**

CETPA Infotech Pvt. Ltd. is a prominent IT services and training company in India, focusing on a variety of activities. It offers corporate training programs designed to enhance the skills of employees in technologies such as Java, Python, .NET, data science, machine learning, and more. The company also specializes in custom software development, providing web, mobile, desktop, and cloud-based applications, along with ERP solutions. CETPA provides industrial training to students in emerging technologies like AI, blockchain, robotics, IoT, and cybersecurity, allowing them to gain hands-on experience. In addition to offline training, CETPA offers online courses and certification programs to help professionals upskill and stay current with industry trends.

They also offer project development support, particularly for technologies like embedded systems and networking. Through internships, workshops, and consultancy services, CETPA aids both students and businesses in navigating digital transformation. Moreover, the company provides placement assistance, helping trainees secure employment in the IT sector. Overall, CETPA's activities aim to bridge the gap between academic knowledge and industry needs by providing practical, technology-driven education and services.

**SUMMER INTERNSHIP AT A GLANCE**

The Summer Internship in Full Stack Development at CETPA Infotech is a 6-week program designed to provide hands-on experience in both front-end and back-end web development. Interns learn technologies like HTML, CSS, JavaScript, React, Node.js, Express.js, and databases such as MongoDB and MySQL. They work on real-time projects, gaining exposure to Agile methodologies, API development, and version control with Git. By the end of the program, interns develop a strong foundation in full stack development and receive placement assistance to help secure jobs in the tech industry.

Interns also have the opportunity to work on capstone projects, earn certifications, and gain insights into industry practices. If you are interested in enhancing your skills in Full Stack Development, this internship is a good opportunity to gain practical exposure.

**MAJOR COUSTOMERS/COMPETITORS**

CETPA Infotech Pvt. Ltd. primarily serves educational institutions, corporate clients, students, professionals, and startups. Its major customers include universities and colleges for providing specialized training programs and internships, businesses seeking corporate training, and students and working professionals looking to enhance their skills in emerging technologies. Additionally, CETPA collaborates with startups needing IT services, custom software development, and digital solutions.

As for competitors, CETPA faces competition from several well-established companies in the IT training and software development sector. Key competitors include NIIT Ltd., which offers a wide range of IT and certification courses; Aptech Ltd., known for its IT and skill development programs; Simplilearn, an online platform offering courses in cloud computing, data science, and full stack development; and TCS iON, Tata Consultancy Services' education and training division.

Online learning platforms like Unacademy and Coursera also compete in the online training space, while HCL Learning, the training arm of HCL Technologies, competes by offering tech-driven education and corporate training solutions. These competitors provide similar services in training, upskilling, and custom software development, targeting students, professionals, and organizations.

**CHAPTER 1**

**INTRODUCTION**

**1.1 Background**

With the growing reliance on full-stack web applications, the integration of frontend and backend technologies has become a fundamental aspect of modern web development. However, this integration often brings forth security challenges, particularly when outdated technologies and practices are used, leaving systems vulnerable to various types of cyberattacks. These risks are amplified when password management and user authentication mechanisms are not implemented securely.

One of the most critical areas of concern is **password handling**. Insecure methods, such as storing passwords in plain text, can lead to devastating breaches if attackers gain access to sensitive data. To ensure the safety of user credentials, **password hashing** and **salting** have become industry-standard practices. Hashing transforms passwords into fixed-length values, while salting adds an additional layer of security by introducing random data before hashing, making it significantly harder for attackers to crack the password.

**1.2 Objectives**

The objective of this report is to design and develop a secure login authentication system using the MERN stack. The system aims to ensure robust password management by utilizing Bcrypt for hashing and salting passwords, thereby protecting sensitive user information. Additionally, the implementation of token-based authentication through JSON Web Tokens (JWT) will provide secure and efficient user sessions. The project aims to:

1.2.1 To develop a secure login authentication system using the MERN stack.

1.2.2 To ensure secure password management by employing Bcrypt for hashing and salting.

1.2.3 To implement token-based authentication using JSON Web Tokens (JWT) for secure user sessions.

1.2.4 To provide users with a seamless and secure experience for registration and login.

1.2.5 To enhance the overall security of the system by protecting sensitive user data.

**1.3 Scope of Project**

The scope includes:

The scope of this project encompasses the development of a secure and efficient user authentication system using the MERN stack. Key aspects of the project scope include:

1. **User Registration and Login:**
   * Enable users to create accounts and log in securely to their profiles.
   * Ensure that the registration and login processes are user-friendly and reliable.
2. **Password Security:**
   * Implement secure password handling using Bcrypt for hashing and salting.
   * Protect sensitive user data by ensuring that passwords are never stored in plaintext.
3. **Token-Based Authentication:**
   * Use JSON Web Tokens (JWT) to manage user authentication and session handling.
   * Ensure secure communication between the client and server by incorporating JWTs in HTTP headers.
4. **Secure Data Flow:**
   * Design the backend to safeguard against common vulnerabilities like SQL injection, XSS, and CSRF.

**1.4 Conclusion**

In conclusion, the development of a secure login authentication system using the MERN stack successfully addresses the critical need for robust user authentication in modern web applications. By employing Bcrypt for hashing and salting, the system ensures secure password storage, mitigating the risks associated with data breaches. Additionally, the integration of JSON Web Tokens (JWT) for token-based authentication provides a reliable mechanism for managing user sessions, enhancing both security and efficiency.

This project demonstrates the effectiveness of combining advanced security techniques with user-centric design to create a seamless and safe registration and login process. The implemented authentication system not only safeguards sensitive user data but also serves as a scalable and secure foundation for future enhancements and integrations within larger web applications.

**CHAPTER 2**

**METHODOLOGY**

**a) Problem Definition**

* When ever we merge two technology like frontend and backend then the developer normally not connect easily.
* When ever the user login and registration our profile at that time there is less secure there personal information.
* Frontend and backend integration can be tricky because they involve different technologies and paradigms. Developers may struggle to connect the React frontend with the Node.js/Express backend efficiently.
* During user login and registration, personal information security is crucial. Inadequate measures to secure this data can expose it to vulnerabilities and breaches.
* Storing passwords in plain text is a major security risk. If a database is compromised, attackers can easily access user credentials.
* Using weak hashing algorithms like MD5 or SHA1 makes it relatively easy for attackers to crack passwords.

**b) Literature Survey**

**[1] S.W. Shah and S. S. Kanhere, "Bcrypt in User Authentication – A Survey," in IEEE Access, vol. 7, pp. 112505-112519, 2023, doi: 10.1109/ACCESS.2023.2932400.**

S.W. Shah and S. S. Kanhere, describes the blind decoding schemes are proposed as tools for protecting customers’ privacy in on-line shopping for electronic documents such that the company has no way of knowing which documents the customers have purchased. Most of the blind decoding schemes suffer from the oracle problem. Schemes utilizing the transformability of digital signatures were proposed to ensure the correctness of the requests from the customers. In this paper, a secure blind decoding scheme based on RSA scheme is proposed. It does not utilize the transformability of RSA digital signature [1].

Niels Provos and David Mazeries, proposes ways of building systems in which password security keeps up with hardware speeds. We formalize the properties desirable in a good password system and show that the computational cost of any secure password scheme must increase as hardware improves. We present two algorithms with adaptable costeksblowsh a block cipher with a purposefully expensive key schedule and bcrypt\_ a related hash function. Failing a major breakthrough in complexity theory these algorithms should allow password based systems to adapt to hardware improvements and remain secure well into the future [2]

Pritesh N, Jigisha K and Paresh V, describes ways of building systems in which password security keeps up with hardware speeds. We formalize the properties desirable in a good password system and show that the computational cost of any secure password scheme must increase as hardware improves. We present two algorithms with adaptable cost a block cipher with a purposefully expensive key schedule and bcrypt a related hash function. Failing a major breakthrough in complexity theory these algorithms should allow password based systems to adapt to hardware improvements and remain secure well into the future.

Thulasimani Lakshmanan and Madheswaran Muthusamy, proposes Hash functions are the most widespread among all cryptographic primitives, and are currently used in multiple cryptographic schemes and in security protocols. The basic design of SHA- 192 is to have the output length of 192.The SHA-192 has been designed to satisfy the different level of enhanced security and to resist the advanced SHA attacks. The security analysis of the SHA-192 is compared to the old one given by NIST and gives more security. The SHA-192 can be used in many applications such s public key cryptosystem, digital sign encryption, message authentication code, random generator and in security architecture of upcoming wireless devices like software defined radio etc [3].

Janaka Deepa kumara, Howard M. Heys and R. Venkatesan, describes message authentication is an essential technique to verify that received messages come from the alleged source and have not been altered.

**[2] Koushik Sen build “Highly scalable, developer-friendly API for the modern web with JavaScript and Node.js” published on 2023 page No.32.**

Planning, generation, and execution of test cases are time-consuming and significantly affected by human errors. In addition, while a software is evolving, APIs are also updated according to current needs. Changes in APIs need to be reflected in test cases. When all these processes (creating requests, entering correct parameters and payload data, creating test data sets, following all changes, and refactoring test cases, executing and reporting tests) are performed manually, testers spend most of their time debugging errors and maintaining the tests. They usually end up having less than necessary number of tests.

This results in suboptimal test coverage, as well as a lack of transparency regarding the quality and quantity of manually performed tests. Testifi is already able to analyse the endpoints of APIs, infer the producer-consumer relationship between endpoints, and create a graph. That helps create a sequence of requests to send to the server to check if the logic behind this sequence is implemented.

The creation of sequences by AI is very limited, as while links between some parameters are found, often not all required values can be provided by AI. This causes manual execution of multiple requests that represent a sequence, which is time consuming. The amount of work required to create and maintain tests could be vastly reduced if the testers were supported with automation and could use tools to create the tests instead of writing them.

Reducing the effort of writing individual tests or performing them manually would also free up resources to improve the quality and coverage of the executed tests and therefore contribute to the quality and speed of future developments.

Regardless of product, enterprise, or domain, software is an inevitable part of the industrial operation. The use of quality software, therefore, is one of the most important aspects of business success in our age. Software testing is an essential quality assurance step used in software development. Testing gives feedback to developers about the quality and functionality of their software so they can correct and optimize their product. Furthermore, testing improves the overall stability of the product and enables the developers to easily add and change features. The later an issue is found the more work is required to fix it. Testing manually is simply not sufficient for modern software development that demands speed and continuous development. Therefore, test automation - tests executed automatically via software tools - is a critical success factor for modern software delivery, and therefore, for modern business. Since web applications are everywhere and modern software development methods employ microservices extensively, test automation for REST APIs is the focus of this project.

**c) Tools And Technology Used**

**Nodemon**

Nodemon is a tool that helps develop Node.js based applications by automatically restarting the node application when file changes in the directory are detected.

Nodemon does not require *any* additional changes to your code or method of development. nodemon is a replacement wrapper for node. To use nodemon, replace the word node on the command line when executing your script.

Nodemon was originally written to restart hanging processes such as web servers, but now supports apps that cleanly exit. If your script exits cleanly, nodemon will continue to monitor the directory (or directories) and restart the script if there are any changes.

If you want to keep all your package configurations in one place, nodemon supports using package.json for configuration. Specify the config in the same format as you would for a config file but under nodemon Config in the package.json file, for example, take the following package.json:

It's generally recommended to use the global nodemon.json to add your own execMap options. However, if there's a common default that's missing, this can be merged in to the project so that nodemon supports it by default, by changing [default.js](https://github.com/remy/nodemon/blob/master/lib/config/defaults.js) and sending a pull request.

Additionally, nodemon does not need any specific modifications to code or the mode of development. It acts as a facilitator in the node by replacing the wrapper for it. To use nodemon, you will simply need to replace the word node on the CLI while you are about to execute your script.

**JWT**

A JSON web token(JWT) is JSON Object which is used to securely transfer information over the web(between two parties). It can be used for an authentication system and can also be used for information exchange. The token is mainly composed of header, payload, signature. These three parts are separated by dots(.).

Authentication and authorization are fundamental aspects of web application security. They ensure that users are who they claim to be and have the right permissions to access specific resources. Traditionally, this was handled through session-based authentication, where user information was stored on the server. However, as applications became more complex and distributed, traditional authentication methods relying on opaque tokens or session-based approaches faced limitations. Validating these tokens often required multiple database lookups and complex server-side logic, leading to performance issues and scalability challenges. The stateful nature of these tokens meant servers had to maintain session information, which could quickly become unwieldy as the number of users and devices grew.

JSON Web Tokens (JWT) are an open standard, which is defined in JSON Web Token (JWT) Specification RFC 7519. They securely represent claims between two parties. Claims can be related to any business process but are typically used to represent an identity and its associations. For example, a user whose identity the JWT represents belongs to an administrator role or group.

The claims in a JWT are encoded as a JSON object and are normally digitally signed with a Message Authentication Code (MAC). The most common scenario for using a JWT is authentication. When the user is logged in, each subsequent request includes the JWT, which allows the user to access services that are permitted by that token.

**Bcrypt**

Bcrypt is a cryptographic hash function designed for password hashing and safe storing in the backend of applications in a way that is less susceptible to dictionary-based cyberattacks. It was created in 1999 by Niels Provos and David Mazières, using the Blowfish cipher algorithm as its base.

Blowfish is notable among block ciphers for its expensive key setup phase. It starts off with subkeys in a standard state, then uses this state to perform a block encryption using part of the key, and uses the result of that encryption (which is more accurate at hashing) to replace some of the subkeys. Then it uses this modified state to encrypt another part of the key, and uses the result to replace more of the subkeys. It proceeds in this fashion, using a progressively modified state to hash the key and replace bits of state, until all subkeys have been set.

Provos and Mazières took advantage of this, and took it further. They developed a new key setup algorithm for Blowfish, dubbing the resulting cipher "Eksblowfish" ("expensive key schedule Blowfish"). The key setup begins with a modified form of the standard Blowfish key setup, in which both the salt and password are used to set all subkeys. There are then a number of rounds in which the standard Blowfish keying algorithm is applied, using alternatively the salt and the password as the key, each round starting with the subkey state from the previous round. In theory, this is no stronger than the standard Blowfish key schedule, but the number of rekeying rounds is configurable; this process can therefore be made arbitrarily slow, which helps deter brute-force attacks upon the hash or salt.

Bcrypt is popular password-hashing library and can be used in various environments. Using bcrypt to hash passwords makes it difficult for attackers to brute-force passwords. As long as the programming language supports the bcrypt library, you can use it to securely hash passwords. For our examples we will be using the bcrypt library with node.js.

Implementing BCrypt in applications involves a few straightforward steps. First, generate a unique salt for each password. Next, hash the password using the BCrypt algorithm along with the salt.

**Postman**

Postman is one of the most popular software testing tools which is used for API testing. With the help of this tool, developers can easily create, test, share, and document APIs.

Why Postman is so famous and what makes it unique when compared to other API testing tools. All the examples in this tutorial are tested and can be imported in Postman.

Postman is a standalone software testing API (Application Programming Interface) platform to build, test, design, modify, and document APIs. It is a simple Graphic User Interface for sending and viewing HTTP requests and responses.

While using Postman, for testing purposes, one doesn't need to write any HTTP client network code. Instead, we build test suites called collections and let Postman interact with the API.

In this tool, nearly any functionality that any developer may need is embedded. This tool has the ability to make various types of HTTP requests like GET, POST, PUT, PATCH, and convert the API to code for languages like JavaScript and Python.

Application Programming Interface (API) is software that acts as an intermediary for two apps to communicate with each other. We use APIs whenever we use an application like Twitter, Facebook, sending text messages, or checking the weather over the phone.

Postman is based on a wide range of extremely user-friendly power tools. For more than 8 million users, Postman has become a tool of convenience.

 Postman is an API(application programming interface) development tool that helps to build, test and modify APIs. Almost any functionality that could be needed by any developer is encapsulated in this tool. It is used by over 5 million developers every month to make their API development easy and simple. It has the ability to make various types of HTTP requests(GET, POST, PUT, PATCH), save environments for later use, converting the API to code for various languages(like JavaScript, and Python).

In essence, Postman transforms the API development landscape by combining versatility, flexibility, simplicity, and efficiency. Whether it’s interacting with APIs, handling authentication, organizing tests, or generating documentation, Postman offers a comprehensive suite of tools tailored to meet the demands of modern software development

Postman stands as an indispensable tool for modern API development, offering a range of features that streamline the development process. Here are key aspects that make Postman a powerful ally in the realm of API development:

**Versatile Request Methods:** Postman supports an array of HTTP request methods, encompassing GET, POST, PUT, DELETE, and PATCH. This versatility allows developers to interact comprehensively with APIs.

**Flexible Request Body Formats:** Developers benefit from the flexibility of handling various request body formats, including form-data, URL-encoded data, raw data, and binary data.

**b) Working Flow Diagram**

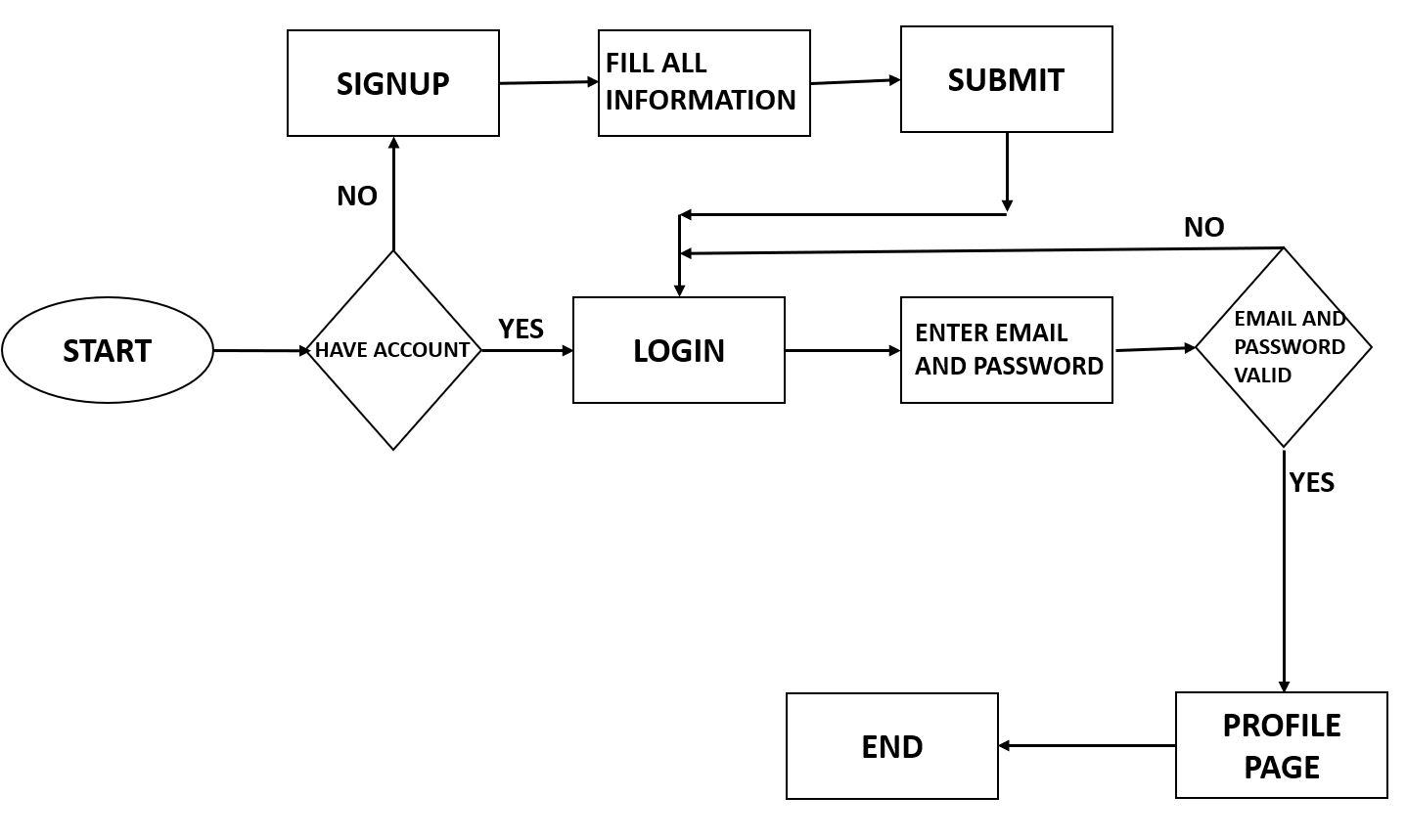
****

Fig 2.1

1. The figure 2.1 is showing whole the project working in which the user first check

the account existent.

2. And then the user if does not any account then they move to the signup button.

3. And then fill the all the information with right and properly so that account are made correctly.

4. And then click the submit button and user automatically move to the home page which is starting page.

**CHAPTER 3**

**SYSTEM DESIGN**

**a) Basic Modules :**

* **User Registration Module :** Allows users to create an account by giving required information such as email, username, and password.
* **User Login Module** : The User Login Module authenticates users using their credentials and generates a secure token (JWT) for session management.
* **Password Management Module :** Encrypts user passwords with bcrypt for secure storage and provides password recovery and reset features.
* **Token Validation Module :** Checks the authenticity of user tokens to prevent unauthorised access.

**b) Data Flow Diagram :**

**c) User Interface Design :**

* **Login Page:** Simple form with fields for email/username and password.
* **Signup Page:** Form with input validation for fields like email, username, and password, confirm password and also allow the terms and condition ensuring a user-friendly experience.
* **Dashboard**: A landing page for authenticated users, displaying personalized content like username, email, and terms and condition in Boolean form and logout functionality.
* **Error Pages**: User-friendly error messages for authentication failures or unauthorized access attempts.

**d) Security Issues :**

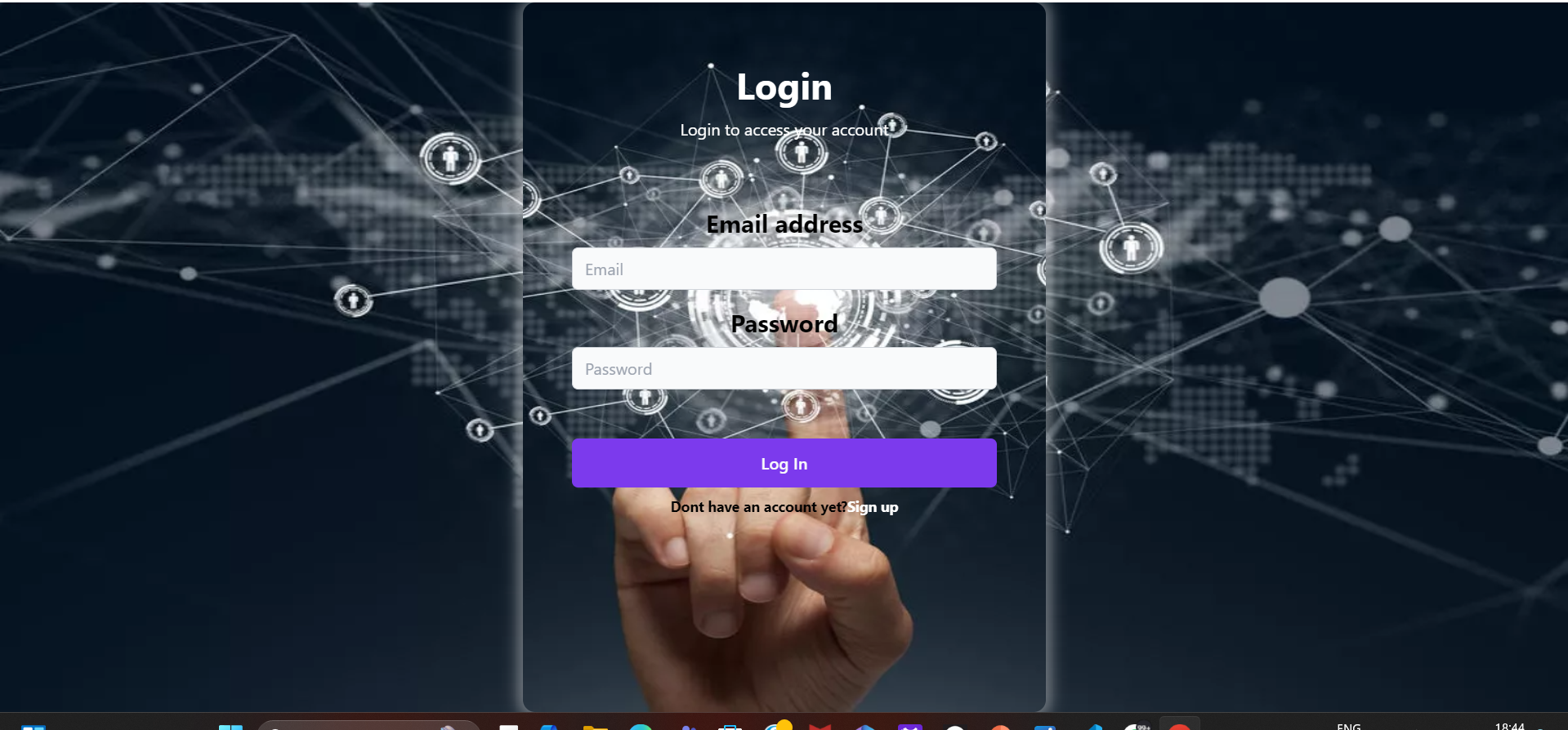
* **Password Storage :** Ensures passwords are securely hashed using bcrypt to prevent leaks.
* **Token Security :** Protects JWTs by implementing secure signing algorithms and setting expiration times.

**CHAPTER 4**

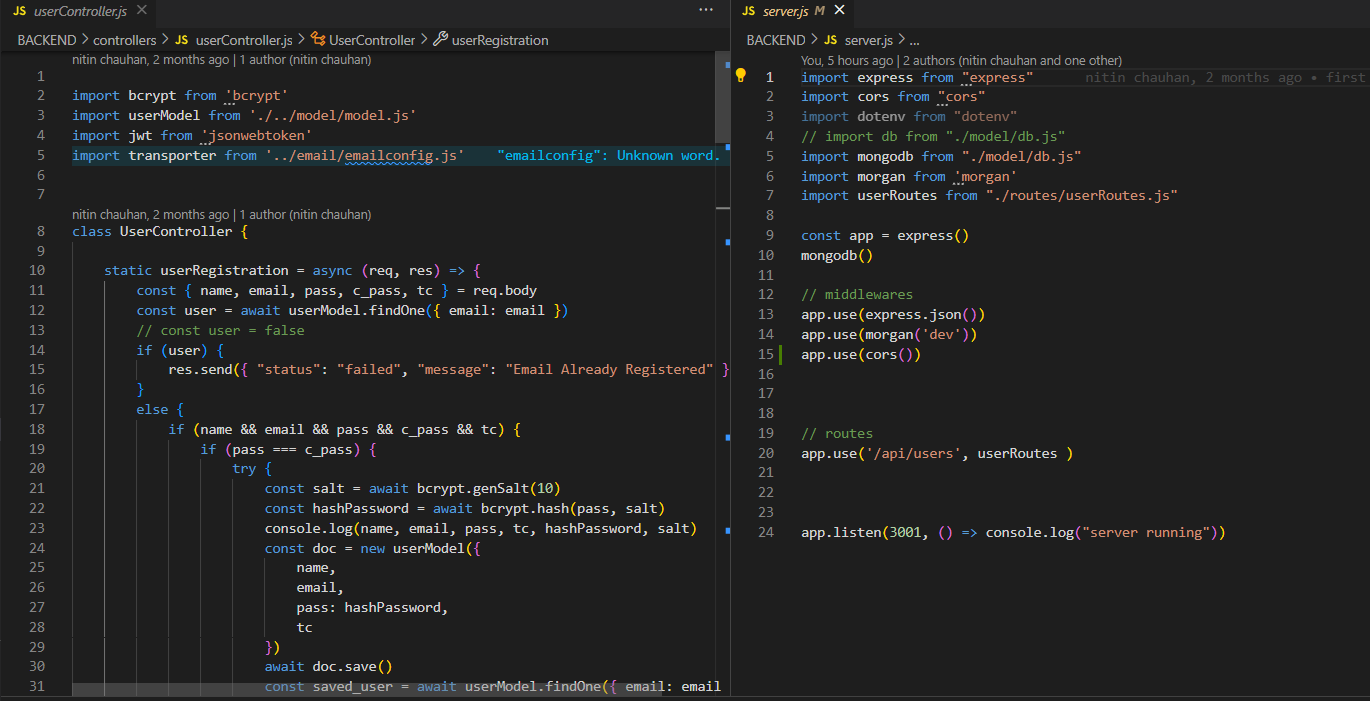
**IMPLEMENTATION AND TEST**

1. **Coding :**

* **Frontend (using React.js) :**
* Created responsive login and signup forms with form validation utilising tools such as React Hook Form.
* API integration was implemented using Axios to connect to backend endpoints.
* Token processing and authentication status are managed in state using React Context or Redux.



* **Backend (Express.js and Node.js) :**
* Created RESTful APIs for token validation, login, and user registration.
* Included JSON Web Tokens (JWT) for safe session management and bcrypt for password hashing.
* Middleware was used to handle errors and validate the API for reliable and secure operation.



* **Database (MongoDB) :**
* Mongoose was used to create schemas for user information, which included hashed password, timestamp, email, and username fields.
* made sure the indexing was correct for quicker lookups and more effective searches.

1. **Testing :**

* **Postman :**
* Postman was used to test API endpoints by sending requests for user registration, login, and token validation to ensure proper functionality. It helped verify responses, error handling, and authentication flow during development.

**CHAPTER 5**

**RESULTS AND DISCUSSION**

1. **Test Reports :**

* **Unit Testing Results :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Module** | **Test Case** | **Expected Output** | **Actual Output** | **Status** |
| Registration | User provides valid input | User registered successfully | Success | Passed |
| Registration | User provides duplicate email | Error message: "Email already exists" | Error displayed | Passed |
| Login | User provides correct credentials | Token generated and returned | Token issued | Passed |
| Login | User provides incorrect password | Error message: "Invalid credentials" | Error displayed | Passed |

* **Integration Testing Results :**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Scenario** | **Steps Performed** | **Expected Outcome** | **Actual Outcome** | **Status** |
| Register a new user and log in | Register → Log in with same credentials | Login successful with JWT | Success | Passed |
| Access protected route without token | Attempt accessing protected route without a token | Access denied | Denied | Passed |
| Logout and access protected route | Log out → Try accessing protected resource | Access denied | Denied | Passed |

**REFERENCE**

[1]Y.C. Chen, G. Horng and C.C. Huang. 2009. Privacy protection in on-line shopping for electronic documents, in: 5th International Conference on Information Assurance and Security, Vol. 2, pp. 105– 108.

[2]Niels Provos and David Mazeries. 1999. “A future – adaptable Password Scheme”, Proceedings of the FREENIX Track: 1999 USENIX Annual Technical Conference, Monterey, California, USA, June 6–11,

[3]Thulasimani Lakshmanan and Madheswaran Muthusamy. 2012. “A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes”, The International Arab Journal of Information Technology, Vol. 9, No. 3, May, pp. 262-267.

[4] Koushik Sen build “Highly scalable, developer-friendly API for the modern web with JavaScript and Node.js” published on 2023 page No.32.