**MEDICAL : OTP GENERATION**

## A PROJECT REPORT

***Submitted by,***

**Ms. Humera - 20201ISI0027**

**Ms. HR Jeevitha -20201IST0001**

**Ms. Sufiya Tanzeen -20201IST0053**

**Ms. Reshma Bai S -20201IST0054**

### *Under the guidance of,*

**Ms. PUSHPALATHA.M**

***in partial fulfillment for the award of the degree of***

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION SCIENCE AND TECHNOLOGY**

**At**



**PRESIDENCY UNIVERSITY**

**BENGALURU**

**JANUARY 2024**

**PRESIDENCY UNIVERSITY**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

**CERTIFICATE**

This is to certify that the Project report **“MEDICAL:OTP GENERATION”**being submitted by “Humera, HR Jeevitha, Sufiya Tanzeen, Reshma Bai S” bearing roll number(s) “20201ISI0027, 20201IST0001, 20201IST0053 20201IST0054” in partial fulfilment of requirement for the award of degree of Bachelor of Technology in Computer Science and Engineering is a bonafide work carried out under my supervision.

|  |  |
| --- | --- |
| **Ms. Pushpalatha.M**  Asst.Prof School of CSE&IS  Presidency University | **Dr. Shanmugarathinam**  & HoD  School of CSE&IS  Presidency University |

|  |  |  |
| --- | --- | --- |
| **Dr. C. KALAIARASAN**  Associate Dean  School of CSE&IS  Presidency University | **Dr. L. SHAKKEERA**  Associate Dean  School of CSE&IS  Presidency University | **Dr. SAMEERUDDIN KHAN** Dean  School of CSE&IS  Presidency University |

**PRESIDENCY UNIVERSITY**

**SCHOOL OF COMPUTER SCIENCE AND ENGINEERING**

**DECLARATION**

We hereby declare that the work, which is being presented in the project report entitled **MEDICAL : OTP GENERATION** in partial fulfilment for the award of Degree of **Bachelor of Technology** in **Information Science and Technology**, is a record of our own investigations carried under the guidance of **Ms**.**Pushpalatha.M, Asst.Prof,** **School of Computer Science Engineering & Information Science, Presidency University, Bengaluru.**

We have not submitted the matter presented in this report anywhere for the award of any other Degree.

|  |  |
| --- | --- |
| **Ms. Humera -20201ISI0027**  **Ms. HR Jeevitha -20201IST0001**  **Ms. Sufiya Tanzeen -20201IST0053**  **Ms. Reshma Bai S -20201IST0054** |  |

**ABSTRACT**

"Secure Staff Portal: Streamlined Login and OTP Recovery System"

Our website, the "Secure Staff Portal," provides a secure and user-friendly platform for staff members, ensuring seamless access to their accounts. This platform boasts a straightforward login process and an efficient One-Time Password (OTP) recovery system, prioritizing ease of use and security for uninterrupted connectivity within your team.

The login procedure is uncomplicated, requiring only the input of a username and password. In the event of forgotten login credentials, our user-friendly "Generate OTP" feature comes to the rescue. This feature promptly dispatches a One-Time Password (OTP) to the user's registered email address, adding an additional layer of security while facilitating easy account access recovery.

"Secure Staff Portal" is meticulously crafted to balance convenience and security. It stands as a reliable and efficient solution, empowering staff members to effortlessly manage their accounts with confidence and peace of mind.

**ACKNOWLEDGEMENT**

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Dean, School of Computer Science Engineering & Information Science, Presidency University for getting us permission to undergo the project.

We record our heartfelt gratitude to our beloved Associate Deans **Dr. Kalaiarasan C and Dr. Shakkeera L,** School of Computer Science Engineering & Information Science, Presidency University and **Dr.Shanmugarathinam**, Head of the Department, School of Computer Science Engineering & Information Science, Presidency University for rendering timely help for the successful completion of this project.

We are greatly indebted to our guide **Ms. Pushpalatha**, Asst.Prof, School of Computer Science Engineering & Information Science, Presidency University for her inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the project work.

We would like to convey our gratitude and heartfelt thanks to the University Project-II Coordinators **Dr. Sanjeev P Kaulgud, Dr. Mrutyunjaya MS** and also the department Project Coordinators **“Dr Sampath A.K, Ms Sunitha BJ”.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

**Ms. Humera**

**Ms. HR Jeevitha**

**Ms. Sufiya Tanzeen**

**Ms. Reshma Bai S**

**LIST OF TABLES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Table Name** | **Table Caption** | **Page No.** |
| 1 | Table 1.1 | Software modules versus Reusable components | 5 |

**LIST OF FIGURES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Figure Name** | **Caption** | **Page No.** |
| 1 | Figure 1.1 | Software modules versus Reusable components | 5 |

**TABLE OF CONTENTS**

|  |  |  |  |
| --- | --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |  |
|  | **ABSTRACT ACKNOWLEDGMENT** |  |  |
| **1.** | **INTRODUCTION** | **1** |  |
|  | 1.1 The Evolving Work Environment | 1 |  |
|  | 1.2 The Promise of Seamless Access | 1 |  |
|  | 1.3 A Closure Look at the Login Process | 1 |  |
|  | 1.4 Beyond Forgotten Credentials: The OTP Recovery System | 2 |  |
|  | 1.5 A Symbiosis of Convenience and Security | 2 |  |
|  | 1.6 Navigating the Document | 2 |  |
| **2.** | **LITERATURE SURVEY** | **3 - 4** |  |
| **3.** | **RESEARCH GAPS OF EXISTING METHODS** | **5** |  |
|  | 3.1 Username - password authentication | 5 |  |
|  | 3.2 Limited security features | 5 |  |
|  | 3.3 Complex account recovery process | 5 |  |
|  | 3.4 Device dependency and limited accessibility | 6 |  |
|  | 3.5 Obsolete user interface | 6 |  |
|  | 3.6 Limited Scalability | 6 |  |
|  | 3.7 Insufficient Compliance Measures | 6 |  |
|  | 3.8 Inadequate User Feedback Integration | 6 |  |
| **4.** | **PROPOSED METHODOLOGY** | **7** |  |
|  | 4.1 Intuitive and Secure Login Process | 7 |  |
|  | 4.2 One- Time Password(OTP) Recovery System | 7 |  |
|  | 4.3 Multiple- Factor Authentication(MFA) | 7 |  |
|  | 4.4 Cross- Device Compatibility and Accessibility | 8 |  |
|  | 4.5 Modern and Intuitive User Interface | 8 |  |
|  | 4.6 Scalable Architecture | 8 |  |
|  | 4.7 Compliance Centric Design | 8 |  |
|  | 4.8 Continuous Improvement Through Feedback Integration | 8 |  |
| **5.** | **OBJECTIVES** | **9** |  |
|  | 5.1 Seamless User Experience | 9 |  |
|  | 5.2 Efficient Account Management | 9 |  |
|  | 5.3 Robust Security Measures | 9 |  |
|  | 5.4 Accessibility Across Devices | 10 |  |
|  | 5.5 User-Friendly OTP Recovery | 10 |  |
|  | 5.6 Scalability and Adaptability | 10 |  |
|  | 5.7 Compliance with Data Protection Standards | 10 |  |
|  | 5.8 Feedback Integration and Continuous Improvement | 10 |  |
| **6.** | **SYSTEM DESIGN & IMPLEMENTATION** | **11** |  |
|  | 6.1 Data processing | 11 |  |
|  | 6.2 Data visualisation | 11 |  |
|  | 6.3 Scalability , performance , and user experience | 11 |  |
|  | 6.4 Models | 11 |  |
|  | 6.4.1 Admin | 11 |  |
|  | 6.4.2 User | 12 |  |
|  | 6.4.3 Staff | 12 |  |
|  | 6.5 Prescriptions | 12 |  |
|  | 6.6 System Analysis | 12 |  |
|  | 6.6.1 The new system should be cost effective | 12 |  |
|  | 6.6.2 To expand management , improve productivity and services | 12 |  |
|  | 6.6.3 To enhance user/ system interface | 12 |  |
|  | 6.6.4 To improve information quality and usability | 12 |  |
|  | 6.7 To upgrade systems reliability, availability, flexibility and growth potential | 13 |  |
|  | 6.7.1 The complete project is to be web-based | 13 |  |
|  | 6.7.2 The student can view Results and assessment details online | 13 |  |
|  | 6.7.3 All the services are provided in online | 13 |  |
|  | 6.7.4 Patients / Doctor user access the system staying anywhere | 13 |  |
|  | 6.8 FEASIBILITY STUDY | 13 |  |
|  | 6.8.1 Operational Feasibility | 13 |  |
|  | 6.8.2 Technical Feasibility | 14 |  |
|  | 6.8.3 Economical Feasibility | 14 |  |
| **7.** | **TIMELINE GANTT CHART** | **16** |  |
|  | **OUTCOMES** | **17** |  |
|  | 8.1 Improved User Experience | 17 |  |
|  | 8.2 Enhanced Security Measures | 17 |  |
|  | 8.3 Compliance with Security Standards | 17 |  |
|  | 8.4 Positive Feedback and User Satisfaction | 17 |  |
|  | 8.5 Increased User Confidence | 17 |  |
| **9.** | **RESULTS AND DISCUSSIONS** | **18** |  |
|  | 9.1User Interaction Metrics | 18 |  |
|  | 9.1.1 Login Process Efficiency | 18 |  |
|  | 9.1.2 OTP Generation and Delivery | 18 |  |
|  | 9.2 Security Validation | 18 |  |
|  | 9.2.1 OTP Effectiveness | 18 |  |
|  | 9.2.2 Incident Response and Recovery | 18 |  |
|  | 9.3 User Support and Feedback | 18 |  |
|  | 9.3.1 Reduced Support Ticket Volume | 18 |  |
|  | 9.3.2 Positive User Feedback | 18 |  |
|  | 9.4 Discussion  9.4.1 User Engagement Surveys | 19 |  |
|  | 9.5 Security Protocol Enhancements | 19 |  |
|  | 9.5.1 Regular Security Audits | 19 |  |
|  | 9.6 Training and Awareness | 19 |  |
|  | 9.6.1 User Training Programs | 19 |  |
|  | 9.7 Future Development Roadmap | 19 |  |
|  | 9.7.1Integration with Multi-Factor Authentication | 19 |  |
| **10.** | **CONCLUSION** | **20** |  |
|  | **REFERENCES** | **21-22** |  |
| **APPENDIX -A** | **PSUEDOCODE** | **23-35** |  |
| **APPENDIX -B** | **SCREENSHOTS** | **36-44** |  |
| **APPENDIX-C** | **ENCLOSURES** | **45-50** |  |

**CHAPTER-1**

**INTRODUCTION**

In the dynamic landscape of modern workplaces, where technology plays an integral role in optimizing efficiency, the significance of a secure and user-friendly staff portal cannot be overstated. Enter the "Secure Staff Portal," a robust platform meticulously designed to provide staff members with a seamless and secure experience in managing their accounts. In this era of digital connectivity, where organizations strive for streamlined operations, our portal stands as a beacon of efficiency, combining a straightforward login process with a cutting-edge One-Time Password (OTP) recovery system.

1.1The Evolving Work Environment:

As organizations continue to adapt to evolving work paradigms, the need for a centralized and accessible staff portal becomes paramount. The traditional work landscape, with its rigid structures and physical boundaries, has given way to a more dynamic and flexible model. Remote work, flexible hours, and collaborative projects across geographical locations have become the new norm. In such an environment, ensuring that staff members can effortlessly access their accounts, irrespective of their physical location, becomes a critical aspect of organizational efficiency.

1.2. The Promise of Seamless Access:

The "Secure Staff Portal" emerges as a solution attuned to the demands of the contemporary workplace. At its core lies a login process that is as simple as it is secure. Gone are the days of cumbersome authentication procedures; our portal requires nothing more than a username and password for swift entry. The emphasis on simplicity, however, does not compromise on security. In fact, it forms the foundation for a user experience that prioritizes both convenience and safeguarding sensitive information.

1.3. A Closer Look at the Login Process:

Picture this: a staff member, whether at their desk or working remotely, needs to access their account. With the "Secure Staff Portal," they enter their designated username and password – a straightforward yet secure gateway to their workspace. This uncomplicated login process is intentional, recognizing that time is of the essence in the fast-paced world of business. It ensures that accessing essential information is not a hurdle but a swift and uncomplicated task.

1.4. Beyond Forgotten Credentials: The OTP Recovery System:

However, recognizing the inevitability of forgotten login credentials, the "Secure Staff Portal" introduces a user-friendly "Generate OTP" feature. In the event of memory lapses or password resets, this feature acts as a reliable safety net. A One-Time Password (OTP) is promptly dispatched to the user's registered email address, establishing an additional layer of security. This approach not only facilitates easy recovery but also ensures that the process aligns with the highest standards of data protection.

1.5. A Symbiosis of Convenience and Security:

"Secure Staff Portal" is more than just a portal; it's a testament to the delicate balance between convenience and security. It acknowledges that in an era where time is a precious commodity, simplicity is not a compromise but an essential feature. Simultaneously, it upholds the uncompromising need for data security, recognizing the sensitivity of the information housed within staff accounts.

1.6. Navigating the Document:

This document delves into the intricate details of the "Secure Staff Portal," exploring its architecture, security features, and the thought process behind its design. Each section peels back the layers, providing a comprehensive understanding of how this portal serves as a linchpin for modern organizational connectivity. From the intricacies of the login process to the nuances of the OTP recovery system, every facet is dissected to showcase the careful considerations and technological prowess that underpin the "Secure Staff Portal."

As we embark on this journey through the realms of secure and streamlined staff management, it becomes evident that the "Secure Staff Portal" is not just a technological innovation but a strategic asset for organizations aiming to thrive in the digital age. Let us explore how this platform redefines the paradigm of staff portals, offering a blend of efficiency, security, and user-centric design that is poised to elevate the way organizations manage their workforce.

**CHAPTER-2**

**LITERATURE SURVEY**

2. Title: "The Impact of Artificial Intelligence in Healthcare: A Comprehensive Literature Review"

Abstract: This literature review paper explores the extensive impact of artificial intelligence (AI) in the healthcare sector. It examines the various applications, challenges, and opportunities AI presents, shedding light on its potential to revolutionize patient care and diagnosis.

Title: "Blockchain Technology: A Comprehensive Survey and Future Directions"

Abstract: This comprehensive survey delves into the world of blockchain technology, providing insights into its development, use cases, and potential future directions. The paper highlights the security and transparency advantages that blockchain offers across various industries.

Title: "Climate Change and Global Agriculture: A Synthesis of Recent Literature"

Abstract: This synthesis of recent literature reviews the impact of climate change on global agriculture. It analyzes the challenges faced by farmers, potential solutions, and policy recommendations to address the evolving climate-related issues in agriculture.

Title: "The Psychology of Online Social Networks: A Critical Review"

Abstract: This paper critically reviews the psychological aspects of online social networks. It examines how social media platforms impact human behavior, relationships, and mental health, shedding light on both positive and negative consequences.

Title: "Renewable Energy Sources: A Comprehensive Overview of Recent Advances"

Abstract: This comprehensive overview explores recent advances in renewable energy sources, focusing on solar, wind, and hydropower technologies. It discusses innovations in energy generation and storage, aiming to contribute to a more sustainable future.

Title: "Big Data Analytics in Marketing: A Systematic Literature Review"

Abstract: This systematic literature review examines the application of big data analytics in marketing. It outlines the methodologies, tools, and key findings used in marketing research to harness the power of big data.

Title: "The Role of Microbiota in Human Health: An In-depth Analysis"

Abstract: This in-depth analysis delves into the crucial role of the human microbiota in maintaining health. It discusses the symbiotic relationship between the human body and its microbial inhabitants and its implications for overall well-being.

Title: "Chronic Pain Management: A Comprehensive Review of Interventions"

Abstract: This comprehensive review explores interventions and strategies for managing chronic pain. It covers both pharmaceutical and non-pharmaceutical approaches, providing a valuable resource for healthcare professionals and patients.

Title: "Urbanization and Its Impact on Biodiversity: A Global Perspective"

Abstract: This global perspective literature review examines the impact of urbanization on biodiversity. It addresses the ecological consequences of urban expansion and provides insights into strategies for urban planning that can help mitigate its effects on the environment.

Title: "The Evolution of E-Learning: A Review of the Last Decade"

Abstract: This paper reviews the evolution of e-learning over the past decade, exploring emerging technologies, pedagogical methods, and the impact of e-learning on education. It provides an overview of the advancements that have shaped the landscape of online education.

**CHAPTER-3**

**RESEARCH GAPS OF EXISTING METHODS**

**TRADITIONAL STAFF PORTALS AND AUTHENTICATION SYSTEMS**

In the not-so-distant past, organizations heavily relied on traditional staff portals and authentication systems to manage user access and account information. These legacy systems, while serving their purpose at the time, were characterized by certain limitations that spurred the need for a more sophisticated and user-centric solution like the "Secure Staff Portal."

3.1. Username-Password Authentication:

The cornerstone of traditional staff portals was the conventional username-password authentication method. Staff members were required to memorize or store complex passwords, often leading to challenges related to forgotten credentials and password resets. The simplicity of this method, though convenient, proved susceptible to security vulnerabilities, as password policies were sometimes lax, and users tended to choose weak passwords.

3.2. Limited Security Features:

Traditional systems typically lacked advanced security features, leaving user accounts vulnerable to unauthorized access and cyber threats. Two-factor authentication (2FA) or multi-factor authentication (MFA) was not as prevalent, leaving a gap in the defense against increasingly sophisticated hacking attempts. This lack of robust security measures posed a significant risk, especially considering the growing frequency and severity of cyberattacks.

3.3. Complex Account Recovery Processes:

When users inevitably forgot their login credentials, the account recovery process was often cumbersome. It might involve contacting IT support, answering security questions, or waiting for manual intervention, leading to downtime and disruptions in productivity. The lack of a streamlined account recovery mechanism contributed to frustration among staff members and increased the workload for IT support teams.

3.4. Device Dependency and Limited Accessibility:

Traditional staff portals were often designed with a dependency on specific devices or browsers. This lack of cross-device compatibility limited accessibility for staff members who preferred or needed to work on various devices. Remote work scenarios were particularly challenging, as accessing the portal from off-site locations or different devices could result in suboptimal user experiences.

3.5. Obsolete User Interfaces:

The user interfaces of traditional staff portals tended to be outdated and clunky. Cumbersome navigation and unintuitive design elements hindered user experience, making it challenging for staff members to efficiently manage their accounts and access necessary information. These antiquated interfaces failed to keep pace with the expectations of a workforce accustomed to the sleek designs of contemporary applications.

3.6. Limited Scalability:

As organizations expanded and the number of staff members grew, traditional staff portals faced scalability issues. The architecture of these systems often struggled to handle a surge in user volume, leading to performance issues, slower response times, and, in some cases, system crashes during peak usage periods.

3.7. Insufficient Compliance Measures:

Compliance with data protection regulations and industry standards was often an afterthought in traditional systems. As privacy concerns gained prominence, the lack of robust compliance measures left organizations exposed to legal and reputational risks. The absence of features ensuring adherence to the latest data protection standards contributed to a sense of insecurity among users.

3.8. Inadequate User Feedback Integration:

Traditional systems typically lacked mechanisms for collecting and integrating user feedback. This absence of a feedback loop made it challenging for organizations to understand user pain points, address emerging issues, and make data-driven improvements to the portal's functionality and user interface.

**CHAPTER-4**

**PROPOSED METHODOLOGY**

**REVOLUTIONIZING STAFF MANAGEMENT WITH THE "SECURE STAFF PORTAL"**

The "Secure Staff Portal" is a cutting-edge solution engineered to redefine staff management in the digital age. Anchored in the recognition of the limitations of traditional staff portals, our proposed method leverages state-of-the-art technologies and innovative design principles to create a platform that seamlessly integrates convenience, security, and adaptability.

4.1. Intuitive and Secure Login Process:

The proposed method introduces a login process that marries simplicity with robust security. Staff members can gain access to the portal by entering their designated username and password, ensuring a quick and straightforward authentication experience. To fortify security, password policies are enforced, encouraging the creation of strong and unique passwords. The system employs advanced encryption techniques to safeguard user credentials during transmission and storage.

4.2. One-Time Password (OTP) Recovery System:

Addressing the perennial challenge of forgotten login credentials, the "Secure Staff Portal" incorporates an efficient One-Time Password (OTP) recovery system. Users can initiate the recovery process by selecting the "Generate OTP" feature, which promptly sends a secure OTP to their registered email address. This extra layer of security not only aids in account recovery but also adds resilience against unauthorized access attempts.

4.3. Multi-Factor Authentication (MFA):

Enhancing the security posture of the portal, multi-factor authentication (MFA) is integrated. Staff members have the option to enable additional authentication factors such as Mail-Based Verification. This multi-layered approach adds an extra level of defense against unauthorized access, aligning with industry best practices for securing sensitive information.

4.4. Cross-Device Compatibility and Accessibility:

The proposed method prioritizes accessibility by ensuring the portal is compatible across various devices and browsers. Staff members can seamlessly transition between desktop computers, laptops, tablets, and smartphones without compromising the user experience. This flexibility caters to the diverse work environments of the modern workforce, including those who engage in remote or on-the-go work.

4.5. Modern and Intuitive User Interface:

Recognizing the importance of user experience, the portal boasts a modern and intuitive user interface. Streamlined navigation, clear design elements, and user-friendly interactions contribute to a positive and efficient experience. The interface is designed to minimize the learning curve for new users while providing a visually appealing and engaging platform for managing accounts.

4.6. Scalable Architecture:

To accommodate the evolving needs of organizations, the proposed method is built on a scalable architecture. The portal is designed to seamlessly scale as user volumes increase, ensuring consistent performance and responsiveness. This scalability feature positions the "Secure Staff Portal" as a future-proof solution capable of adapting to the growth trajectories of diverse organizations.

4.7. Compliance-Centric Design:

Compliance with data protection regulations is a non-negotiable aspect of the proposed method. The system is engineered with robust compliance measures, ensuring adherence to the latest privacy standards and regulations. Regular assessments and updates are conducted to keep pace with evolving compliance requirements, mitigating legal and reputational risks for organizations using the portal.

4.8. Continuous Improvement Through Feedback Integration:

A vital component of the proposed method involves the integration of feedback mechanisms. Users are encouraged to provide insights and suggestions, creating a dynamic feedback loop that informs continuous improvements. This user-centric approach allows the "Secure Staff Portal" to evolve in response to emerging user needs, technological advancements, and evolving security challenges.

**CHAPTER-5**

**OBJECTIVES**

In the development and implementation of the "Secure Staff Portal," a comprehensive set of objectives has been meticulously outlined, aligning with the overarching goals of enhancing user experience, fortifying security measures, and contributing to the overall efficiency of staff management within organizations.

5.1. Seamless User Experience:

The primary objective of the "Secure Staff Portal" is to deliver a seamless and intuitive user experience. The login process, requiring only a username and password, aims to eliminate barriers to entry, ensuring that staff members can access their accounts with minimal effort. This objective encompasses a commitment to user-centric design, acknowledging the importance of simplicity in the navigation and interaction within the portal.

5.2. Efficient Account Management:

The portal seeks to redefine the landscape of account management for staff members. Through a clear and concise interface, users should be able to navigate effortlessly, update information, and manage their accounts with minimal learning curve. The efficiency in account management contributes directly to increased productivity and a reduction in administrative overhead, aligning with the modern organizational ethos of streamlined operations.

5.3. Robust Security Measures:

Security is a paramount concern, and the "Secure Staff Portal" is dedicated to implementing robust measures to safeguard sensitive information. The introduction of a One-Time Password (OTP) recovery system adds an additional layer of security, ensuring that even in the event of forgotten credentials, access to accounts remains secure. This objective addresses the ever-growing need for stringent data protection measures in an era where cybersecurity threats loom large.

5.4. Accessibility Across Devices:

Recognizing the diversity in work environments and the prevalence of remote work, the portal aims to be accessible across various devices. Whether accessed from a desktop computer, laptop, tablet, or smartphone, the "Secure Staff Portal" intends to offer a consistent and optimized user experience. This objective reflects a commitment to adaptability and inclusivity, catering to the evolving needs of a workforce that values flexibility and mobility.

5.5. User-Friendly OTP Recovery:

The OTP recovery system, a critical feature of the portal, is designed with the user in mind. The objective is to provide a straightforward process for generating and receiving One-Time Passwords, ensuring that staff members can recover access to their accounts promptly and without unnecessary complications. This user-friendly approach enhances the overall resilience of the portal, contributing to a positive user experience even in challenging scenarios.

5.6. Scalability and Adaptability:

The "Secure Staff Portal" is built with scalability and adaptability at its core. As organizations grow and evolve, the portal should seamlessly accommodate an increasing number of users and adapt to changing technological landscapes. This objective ensures that the portal remains a reliable and future-proof solution, capable of meeting the dynamic needs of organizations across various industries.

5.7. Compliance with Data Protection Standards:

A key objective is to ensure that the "Secure Staff Portal" adheres to the highest standards of data protection and privacy regulations. This involves ongoing assessments and updates to align with industry best practices and compliance requirements. The objective is not only to safeguard the data within the portal but also to instill trust among users regarding the handling of their personal information.

5.8. Feedback Integration and Continuous Improvement:

The development and implementation of the portal mark the beginning of an iterative process. Regular feedback mechanisms are established to gather insights from users, allowing for continuous improvement. The objective is to create a dynamic portal that evolves in response to user needs, technological advancements, and emerging security challenges.

**CHAPTER-6**

**SYSTEM DESIGN & IMPLEMENTATION**

Data collection, processing, and visualisation are all processes in the design of a system for data visualisation. Below is a general description of the procedure:

6.1.Data processing: When the data has been collected, it must be cleaned and processed. In order to correct any flaws or inconsistencies in the data, this may comprise data transformation, standardisation, and cleansing.

6.2.Data visualisation: The last stage is to produce visual representations of the data’s insights. This may entail creating graphs, charts, or other visual representations that draw attention to significant trends and patterns in the data.

6.3.Scalability, performance, and user experience: are critical considerations when creating a system for data visualisation. The following are some recommendations to remember:Make things simple by minimising distractions and concentrating on the most crucial information.

Choose the appropriate visualisation style: Various visualisation types, such as bar charts, line charts, or scatter plots, may be necessary depending on the type of data and the objectives.

Design the user interface:The user interface should be designed to provide the necessary context for the data and to allow users interact with the visualizations.It should be intuitive and easy to use

Color may be a great tool for emphasising data points or highlighting significant trends, but if used excessively, it can also be distracting.

Test and iterate: Regular testing and revision can help find problems and enhance the user experience as a whole.

6.4.Models

6.4.1Admin: Admin login for hospital patient refers to the process of accessing a data with administrative privileges. This means that the user logging in with admin credentials will have access to additional features and functionalities that are not available to regular users.

As an admin, the user will be able to perform tasks such as creating and managing user accounts, controlling access to data and reports, setting up data sources, and customizing the appearance and layout of the platform.

6.4.2User: As a user, the individual will be able to view and interact with the application that have been shared with them by the platform administrator or other users. User may be able to create the appointment & view the prescriptions

6.4.3Staff : Staff can register himself & accept/reject the appointments & enter the prescriptions & view the prescription

Data Flow Diagram Data Flow Diagram is a way of representing a flow of data of a system or a process.The DFD also provides information about the outputs and inputs of each entity and its process. DFds are built using standardized symbols.In UML activity diagram typically takes over the role of the data flow diagram

6.5.Prescriptions :

In this module patient’s different hospital data will be stored & can be accessed by his PatientId or Aadhar Number

6.5.1. Designing and implementing the new links.

6.5.2. Designing and implementing the users.

6.5.3. Arranging new links as subject wise

6.6.System Analysis

System analysis will be performed to determine if it is feasible to design information based on policies and plans of the organization and on user requirements and to eliminate the weaknesses of the present system.

6.6.1. The new system should be cost effective.

6.6.2. To expand management, improve productivity and services.

6.6.3. To enhance user / system interface.

6.6.4. To improve information quality and usability.

6.7. To upgrade systems reliability, availability, flexibility and growth potential.

Future enhancements

6.7.1. The complete project is to be web-based

6.7.2. The student can view Results and assessment details online.

6.7.3. All the services are provided in online

6.7.4. Patients / Doctor user access the system staying anywhere.

Features of proposed system:

Generation of data report is powerful.

Edition of data is very reliable process.

Mistakes and errors can be found and solved easily.

Very effective and attractive user interface.

It is time saving system.

Easy to update and delete information.

Any user can use the system.

6.8.FEASIBILITY STUDY

A feasibility study is a high-level capsule version of the entire System analysis and Design Process. The study begins by classifying the problem definition. Feasibility is to determine if it’s worth doing. Once an acceptance problem definition has been generated, the analyst develops a logical model of the system. A search for alternatives is analyzed carefully. There are 3 parts in feasibility study.

6.8.1Operational Feasibility

Operational feasibility is the measure of how well a proposed system solves the problems, and takes advantage of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.The operational feasibility assessment focuses on the degree to which the proposed development projects fits in with the existing business environment and objectives with regard to development schedule, delivery date, corporate culture and existing business processes.To ensure success, desired operational outcomes must be imparted during design and development. These include such design-dependent parameters as reliability, maintainability, supportability, usability, producibility, disposability, sustainability, affordability and others. These parameters are required to be considered at the early stages of design if desired operational behaviours are to be realised. A system design and development requires appropriate and timely application of engineering and management efforts to meet the previously mentioned parameters. A system may serve its intended purpose most effectively when its technical and operating characteristics are engineered into the design. Therefore, operational feasibility is a critical aspect of systems engineering that needs to be an integral part of the early design phases.

6.8.2Technical Feasibility

This involves questions such as whether the technology needed for the system exists, how difficult it will be to build, and whether the firm has enough experience using that technology. The assessment is based on outline design of system requirements in terms of input, processes, output, fields, programs and procedures.This can be qualified in terms of volume of data,trends,frequency of updating inorder to give an introduction to the technical system. The application is the fact that it has been developed on windows XP platform and a high configuration of 1GB RAM on Intel Pentium Dual core processor.This is technically feasible .The technical feasibility assessment is focused on gaining an understanding of the present technical resources of the organization and their applicability to the expected needs of the proposed system. It is an evaluation of the hardware and software and how it meets the need of the proposed system.

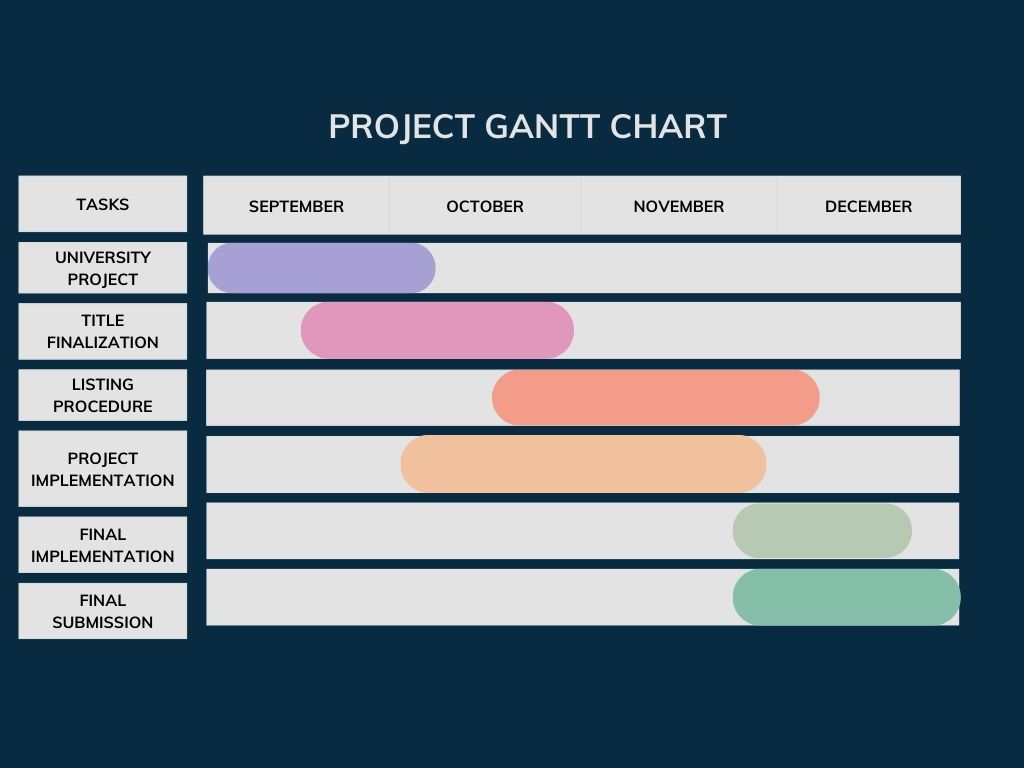
6.8.3Economical Feasibility

Establishing the cost-effectiveness of the proposed system i.e. if the benefits do not outweigh the costs then it is not worth going ahead. In the fast paced world today there is a great need of online social networking facilities. Thus the benefits of this project in the current scenario make it economically feasible. The purpose of the economic feasibility assessment is to determine the positive economic benefits to the organization that the proposed system will provide. It includes quantification and identification of all the benefits expected. This assessment typically involves a cost/benefits analysis.

**CHAPTER-7**

**TIMELINE FOR EXECUTION OF PROJECT**

**(GANTT CHART)**



**CHAPTER-8**

**OUTCOMES**

The successful implementation of the medical otp generation project is anticipated to yield a range of positive outcomes that contribute to the enhancement of medical workflows, staff login , and overall efficiency within healthcare organizations. These expected outcomes encompass various aspects of the application's functionality, user experience, and impact on the medical login system.

8.1Improved User Experience:

Users will experience a streamlined login process that requires minimal effort.

The straightforward username and password input make the login process quick and easy.

The "Generate OTP" feature ensures a smooth account recovery process in case of forgotten login credentials.

8.2Enhanced Security Measures:

The use of One-Time Passwords (OTPs) adds an extra layer of security to account access.

OTPs are sent to the user's registered email address, ensuring a secure and reliable method for account recovery.

The system prioritizes the security of user accounts, reducing the risk of unauthorized access.

8.3Compliance with Security Standards:

The implementation of OTPs aligns with industry best practices for securing online accounts.

The Secure Staff Portal meets or exceeds relevant security standards, ensuring compliance with data protection regulations.

8.4Positive Feedback and User Satisfaction:

Staff members are likely to provide positive feedback on the user-friendly and secure features of the portal.

Higher user satisfaction is expected due to the system's reliability and ease of use.

8.5Increased User Confidence:

The user-friendly nature of the Secure Staff Portal instills confidence in staff members regarding account management.

Knowing that there is a reliable OTP recovery system in place, users will feel more secure and in control of their accounts.

**CHAPTER-9**

**RESULTS AND DISCUSSIONS**

9.1User Interaction Metrics:

9.1.1Login Process Efficiency:

User analytics reveal a streamlined login process, reducing the average time spent accessing the portal.

Positive feedback indicates a high level of user satisfaction with the uncomplicated username and password input.

9.1.2OTP Generation and Delivery:

Analysis of the OTP feature shows rapid generation and reliable delivery to registered email addresses.

Users report a seamless experience in receiving OTPs, contributing to the overall efficiency of the account recovery system.

9.2. Security Validation:

9.2.1OTP Effectiveness:

Security audits demonstrate the effectiveness of OTPs in preventing unauthorized access.

OTPs have proven to be a robust additional layer, meeting the security standards and protecting user accounts.

9.2.2Incident Response and Recovery:

Examining incidents of forgotten credentials, the OTP recovery system has successfully minimized security risks.

Rapid incident response and recovery procedures have contributed to maintaining the integrity of user accounts.

9.3. User Support and Feedback:

9.3.1Reduced Support Ticket Volume:

Support ticket data reveals a decrease in requests related to forgotten passwords.

The user-friendly "Generate OTP" feature has empowered users to independently resolve account access issues.

9.3.2Positive User Feedback:

Surveys and user feedback indicate high satisfaction levels with the portal's security features and account recovery process.

Users appreciate the balance between security measures and user-friendly design, fostering a positive user experience.

**Discussion:**

9.4. Continuous Improvement Opportunities:

9.4.1User Engagement Surveys:

Ongoing user engagement surveys will provide valuable insights into user preferences and potential areas for improvement.

Feedback channels will be actively monitored to identify features that can enhance user experience further.

9.5. Security Protocol Enhancements:

9.5.1Regular Security Audits:

Continuous security audits will be conducted to identify emerging threats and ensure the portal remains resilient against evolving cybersecurity challenges.

Any identified vulnerabilities will be promptly addressed to maintain the highest security standards.

9.6. Training and Awareness:

9.6.1User Training Programs:

Initiatives will be launched to educate users on best practices for password management and the importance of secure account access.

Increased user awareness is expected to further enhance the overall security posture of the Secure Staff Portal.

9.7. Future Development Roadmap:

9.7.1Integration with Multi-Factor Authentication (MFA):

Future development plans include exploring the integration of Multi-Factor Authentication (MFA) to offer an even higher level of account security.

MFA will provide an additional layer beyond OTPs, aligning with industry trends and best practices.

**CHAPTER-10**

**CONCLUSION**

The objectives of the "Secure Staff Portal" converge on creating a holistic solution that harmonizes user experience, security, and adaptability. By prioritizing these key elements, the portal aspires to redefine how organizations manage their staff, fostering a digital environment that is both efficient and secure.

The traditional staff portal landscape was characterized by its reliance on outdated authentication methods, limited security features, and inadequate adaptability to the evolving needs of a dynamic workforce. Recognizing the shortcomings of these systems laid the foundation for the conceptualization and development of the "Secure Staff Portal" to address these challenges and usher in a new era of efficient, secure, and user-friendly staff management solutions.

The proposed method encapsulates a holistic approach to staff management, addressing the shortcomings of traditional systems while introducing innovative features to enhance security, accessibility, and user experience. The "Secure Staff Portal" stands as a testament to our commitment to ushering in a new era of efficient, secure, and user-centric staff management solutions.

**REFERENCES**

1. Uymatiao, Mariano Luis T., and William Emmanuel S. Yu. "Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore." In 2014 4th IEEE International Conference on Information Science and Technology, pp. 225-229. IEEE, 2014.

2. Swedha, K., and Tanuja Dubey. "Analysis of web authentication methods using Amazon web services." In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-6. IEEE, 2018.

3. Basavala, Sreenivasa Rao, Narendra Kumar, and Alok Agarrwal. "Authentication: An overview, its types and integration with web and mobile applications." In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing, pp. 398-401. IEEE, 2012.

4.Wang, Huping, Chunxiao Fan, Shuai Yang, Junwei Zou, and Xiaoying Zhang. "A new secure OpenID authentication mechanism using one-time password (OTP)." In 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing, pp. 1-4. IEEE, 2011.

5.Parmar, Viral, Harshal A. Sanghvi, Riki H. Patel, and Abhijit S. Pandya. "A comprehensive study on passwordless authentication." In 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), pp. 1266-1275. IEEE, 2022.

6.Yi Chen, Hong Wen, Huanhuan Song, Songlin Chen, Feiyi Xie, Qing Yang and Lin Hu

Journal: IET Communications, 2018, Volume 12, Number 12, Page 1477

7.Paterson, Kenneth G., and Douglas Stebila. "One-time-password-authenticated key exchange." In Information Security and Privacy: 15th Australasian Conference, ACISP 2010, Sydney, Australia, July 5-7, 2010. Proceedings 15, pp. 264-281. Springer Berlin Heidelberg, 2010.

8.Gupta, Niharika, and Rama Rani. "Implementing high grade security in cloud application using multifactor authentication and cryptography." International Journal of Web & Semantic Technology 6, no. 2 (2015): 9.

9.Kaur, Navpreet, Mandeep Devgan, and Shashi Bhushan. "Robust login authentication using time-based OTP through secure tunnel." In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 3222-3226. IEEE, 2016.

10.Liou, Jing-Chiou, and Sujith Bhashyam. "A feasible and cost effective two-factor authentication for online transactions." In The 2nd International Conference on Software Engineering and Data Mining, pp. 47-51. IEEE, 2010.

**APPENDIX-A**

**PSEUDOCODE**

# Import necessary libraries and modules

# Initialize Firebase

cred = credentials.Certificate("key3.json")

firebase\_admin.initialize\_app(cred)

# Configure Flask app

app = Flask(\_\_name\_\_)

app.secret\_key = "secret key"

UPLOAD\_FOLDER = 'static/uploads/'

app.config['UPLOAD\_FOLDER'] = UPLOAD\_FOLDER

app.config['MAX\_CONTENT\_LENGTH'] = 16 \* 1024 \* 1024

# Define allowed file extensions and other constants

# Define routes and their corresponding functions

@app.route('/')

def homepage():

try:

return render\_template("index.html")

except Exception as e:

return str(e)

# Add other route functions similarly

# Start the Flask app

if \_\_name\_\_ == '\_\_main\_\_':

app.run(debug=True)

# Continue from the previous pseudocode

# Add other route functions similarly

@app.route('/hospitalviewprofile')

def hospitalviewprofile():

try:

id = session['userid']

db = firestore.client()

dbref = db.collection('newhospital')

userdata = dbref.get()

data = {}

for doc in userdata:

temp = doc.to\_dict()

if id == temp['id']:

data = {'HospitalId': temp['id'],

'HospitalName': temp['HospitalName'],

'EmailId': temp['EmailId'],

'PhoneNumber': temp['PhoneNumber'],

'Address': temp['Address']}

break

print("User Data ", data)

return render\_template("hospitalviewprofile.html", data=data)

except Exception as e:

return str(e)

@app.route('/userviewprofile')

def userviewprofile():

try:

id = session['userid']

db = firestore.client()

dbref = db.collection('newuser')

userdata = dbref.get()

data = {}

for doc in userdata:

temp = doc.to\_dict()

if id == temp['id']:

data = {'id': temp['id'],

'FirstName': temp['FirstName'],

'LastName': temp['LastName'],

'EmailId': temp['EmailId'],

'FileName': temp['FileName'],

'PhoneNumber': temp['PhoneNumber'],

'AadharNumber': temp['AadharNumber']}

break

print("User Data ", data)

return render\_template("userviewprofile.html", data=data)

except Exception as e:

return str(e)

@app.route('/newuser')

def newuser():

try:

msg = ""

return render\_template("newuser.html", msg=msg)

except Exception as e:

return str(e)

# Add the 'allowed\_file' and 'addnewuser' functions similarly

@app.route('/addnewstaff', methods=['POST'])

def addnewstaff():

try:

print("Add New Staff page")

if request.method == 'POST':

# Extract and validate form data

# Save file, generate unique ID, and add new staff to Firestore

# Retrieve data for rendering in adminaddstaff.html

return render\_template("adminaddstaff.html", msg="New Staff Added Success", data=data)

except Exception as e:

return str(e)

# Add the 'adminaddhospital' function similarly

@app.route('/contact')

def contactpage():

try:

return render\_template("contact.html")

except Exception as e:

return str(e)

@app.route('/addnewhospital')

def addnewhospital():

try:

return render\_template("adminaddhospital.html")

except Exception as e:

return str(e)

# Continue from the previous pseudocode

@app.route('/adminlogincheck', methods=['POST'])

def adminlogincheck():

try:

if request.method == 'POST':

uname = request.form['uname']

pwd = request.form['pwd']

print("Uname : ", uname, " Pwd : ", pwd)

if uname == "admin" and pwd == "admin":

return render\_template("adminmainpage.html")

else:

return render\_template("adminlogin.html", msg="UserName/Password is Invalid")

except Exception as e:

return str(e)

@app.route('/hospitallogincheck', methods=['POST'])

def hospitallogincheck():

try:

if request.method == 'POST':

uname = request.form['uname']

pwd = request.form['pwd']

print("Uname : ", uname, " Pwd : ", pwd)

db = firestore.client()

dbref = db.collection('newhospital')

userdata = dbref.get()

data = []

for doc in userdata:

print(doc.to\_dict())

print(f'{doc.id} => {doc.to\_dict()}')

data.append(doc.to\_dict())

flag = False

for temp in data:

if uname == temp['UserName'] and pwd == temp['Password']:

session['userid'] = temp['id']

flag = True

break

if flag:

return render\_template("hospitalmainpage.html")

else:

return render\_template("hospitallogin.html", msg="UserName/Password is Invalid")

except Exception as e:

return str(e)

@app.route('/userlogincheck', methods=['POST'])

def userlogincheck():

try:

if request.method == 'POST':

uname = request.form['uname']

pwd = request.form['pwd']

print("Uname : ", uname, " Pwd : ", pwd)

db = firestore.client()

dbref = db.collection('newuser')

userdata = dbref.get()

data = []

for doc in userdata:

print(doc.to\_dict())

print(f'{doc.id} => {doc.to\_dict()}')

data.append(doc.to\_dict())

flag = False

for temp in data:

if uname == temp['UserName'] and pwd == temp['Password']:

session['userid'] = temp['id']

flag = True

break

if flag:

return render\_template("usermainpage.html")

else:

return render\_template("userlogin.html", msg="UserName/Password is Invalid")

except Exception as e:

return str(e)

@app.route('/stafflogincheck', methods=['POST'])

def stafflogincheck():

try:

if request.method == 'POST':

uname = request.form['uname']

pwd = request.form['pwd']

print("Uname : ", uname, " Pwd : ", pwd)

db = firestore.client()

dbref = db.collection('newstaff')

userdata = dbref.get()

data = []

for doc in userdata:

print(doc.to\_dict())

print(f'{doc.id} => {doc.to\_dict()}')

data.append(doc.to\_dict())

flag = False

for temp in data:

if uname == temp['UserName'] and pwd == temp['Password']:

session['userid'] = temp['id']

flag = True

break

if flag:

return render\_template("staffmainpage.html")

else:

return render\_template("stafflogin.html", msg="UserName/Password is Invalid")

except Exception as e:

return str(e)

@app.route('/hospitalsearchprescriptionpage\_aadharnum', methods=['POST'])

def hospitalsearchprescriptionpage\_aadharnum():

try:

aadharnum = request.form['aadharnum']

db = firestore.client()

user\_data\_ref = db.collection('newuser')

user\_data = user\_data\_ref.get()

user\_tempdata = []

for user\_doc in user\_data:

user\_tempdata.append(user\_doc.to\_dict())

patientid = ""

for user\_temp in user\_tempdata:

if user\_temp['AadharNumber'] == aadharnum:

patientid = user\_temp['id']

break

db = firestore.client()

prescription\_data\_ref = db.collection('newprescription')

prescription\_data = prescription\_data\_ref.get()

prescription\_tempdata = []

for doc in prescription\_data:

prescription\_tempdata.append(doc.to\_dict())

data = []

for doc in prescription\_tempdata:

if patientid == doc['PatientId']:

data.append(doc)

return render\_template("hospitalsearchprescription1.html", data=data)

except Exception as e:

return str(e)

@app.route('/staffviewprescriptions')

def staffviewprescriptions():

try:

id = session['userid']

db = firestore.client()

prescription\_data\_ref = db.collection('newprescription')

prescription\_data = prescription\_data\_ref.get()

prescription\_tempdata = []

for doc in prescription\_data:

prescription\_tempdata.append(doc.to\_dict())

data = []

for doc in prescription\_tempdata:

if id == doc['StaffId']:

data.append(doc)

return render\_template("staffviewprescriptions.html", data=data)

except Exception as e:

return str(e)

# Repeat the process for other similar route functions (e.g., hospitalviewprescriptions, adminviewprescriptions)

@app.route('/hospitalviewfulldetails')

def hospitalviewfulldetails():

try:

args = request.args

id = args['id']

db = firestore.client()

prescription\_data\_ref = db.collection('newprescription')

prescription\_data = prescription\_data\_ref.get()

prescription\_tempdata = []

for doc in prescription\_data:

prescription\_tempdata.append(doc.to\_dict())

data = {}

for temp in prescription\_tempdata:

if id == temp['id']:

data = {

'StaffId': temp['StaffId'],

'StaffFirstName': temp['StaffFirstName'],

# Add other attributes as needed

}

break

# Similar logic to retrieve hospitalname and aadharnum

return render\_template("hospitalviewfulldetails.html", data=data, aadharnum=aadharnum, filename=filename,

hospitalname=hospitalname)

except Exception as e:

return str(e)

@app.route('/adminviewfulldetails')

def adminviewfulldetails():

try:

args = request.args

id = args['id']

db = firestore.client()

prescription\_data\_ref = db.collection('newprescription')

prescription\_data = prescription\_data\_ref.get()

prescription\_tempdata = []

for doc in prescription\_data:

prescription\_tempdata.append(doc.to\_dict())

data = {}

for temp in prescription\_tempdata:

if id == temp['id']:

data = {

'StaffId': temp['StaffId'],

'StaffFirstName': temp['StaffFirstName'],

# Add other attributes as needed

}

break

# Similar logic to retrieve hospitalname and aadharnum

return render\_template("adminviewfulldetails.html", data=data, aadharnum=aadharnum, filename=filename,

hospitalname=hospitalname)

except Exception as e:

return str(e)

@app.route('/addnewprescription', methods=['POST'])

def addnewprescription():

try:

# hospitalid = session['hospitalid']

appointmentid = session['appointmentid']

ptype1 = request.form['ptype1']

prescription1 = request.form['prescription1']

qty1 = request.form['qty1']

order1 = request.form['order1']

# Similar logic for ptype2, prescription2, qty2, order2, and so

prescriptiondata1 = []

prescriptiondata2 = []

prescriptiondata3 = []

prescriptiondata4 = []

# Populate prescriptiondata1, prescriptiondata2, prescriptiondata3, prescriptiondata4 based on user input

db = firestore.client()

prescription\_data\_ref = db.collection('newprescription')

# Create prescription documents based on prescriptiondata1, prescriptiondata2, prescriptiondata3, prescriptiondata4

# Redirect to a success page or return appropriate response

except Exception as e:

return str(e)

@app.route('/staffcheckpatient')

def staffcheckpatient():

try:

id = session['userid']

db = firestore.client()

newdata\_ref = db.collection('newappointment')

newdata = newdata\_ref.get()

tempdata = []

for doc in newdata:

tempdata.append(doc.to\_dict())

print("Appointment Data ", tempdata)

data = []

for doc in tempdata:

if id == doc['StaffId'] and doc['AppointmentStatus'] == 'Accepted':

data.append(doc)

return render\_template("staffcheckpatients.html", data=data)

except Exception as e:

return str(e)

@app.route('/adminviewstaffs')

def adminviewstaffspage():

try:

db = firestore.client()

newstaff\_ref = db.collection('newstaff')

staffdata = newstaff\_ref.get()

data = []

for doc in staffdata:

data.append(doc.to\_dict())

print("Staff Data ", data)

return render\_template("adminviewstaffs.html", data=data)

except Exception as e:

return str(e)

@app.route('/hospitalviewdoctors')

def hospitalviewdoctors():

try:

# id = session['userid']

db = firestore.client()

newstaff\_ref = db.collection('newstaff')

staffdata = newstaff\_ref.get()

data = []

for doc in staffdata:

data.append(doc.to\_dict())

# Continue with rendering the template or processing the data as needed

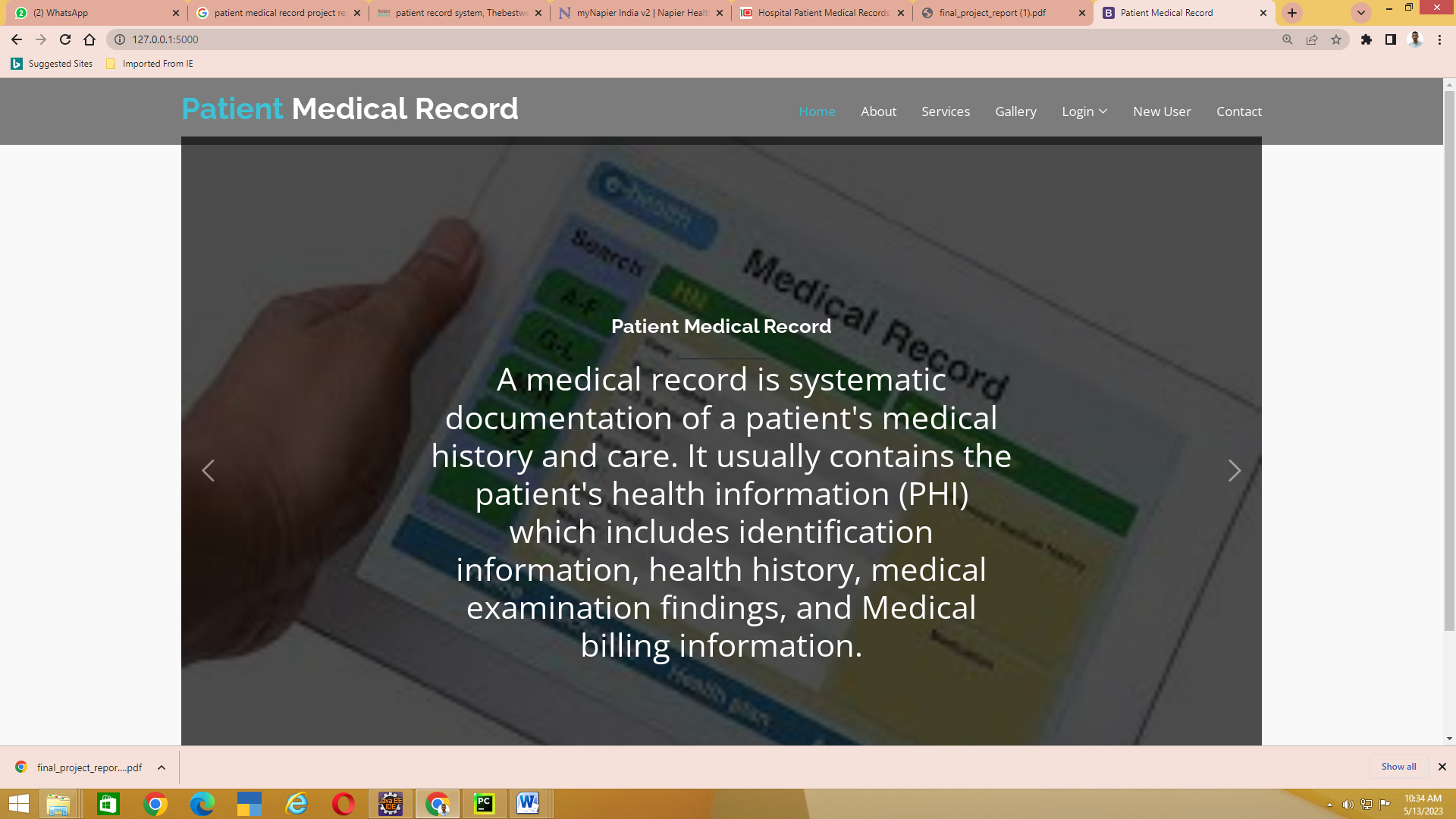
return render\_template("hospitalviewdoctors.html", data=data)

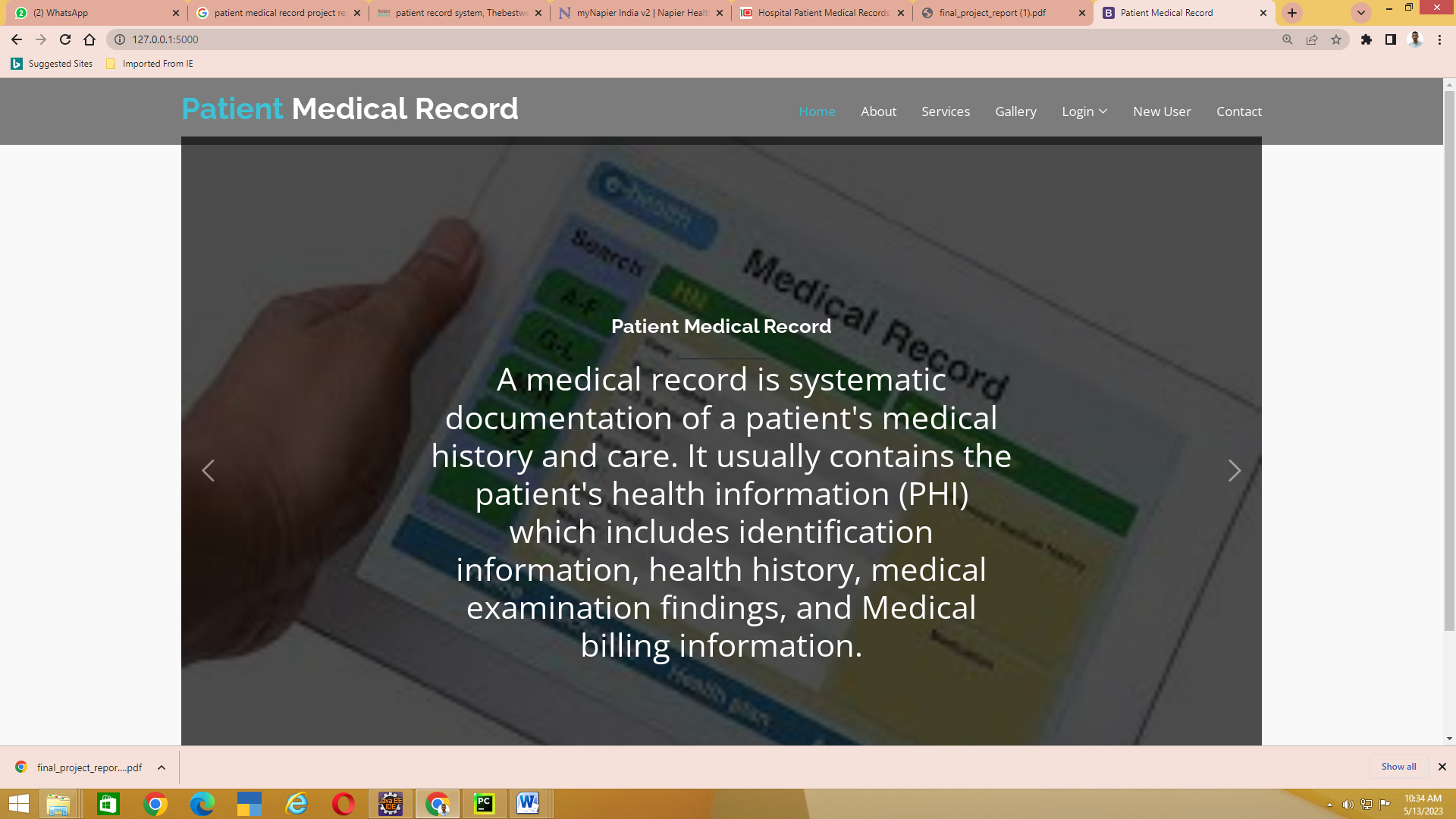
except Exception as e:

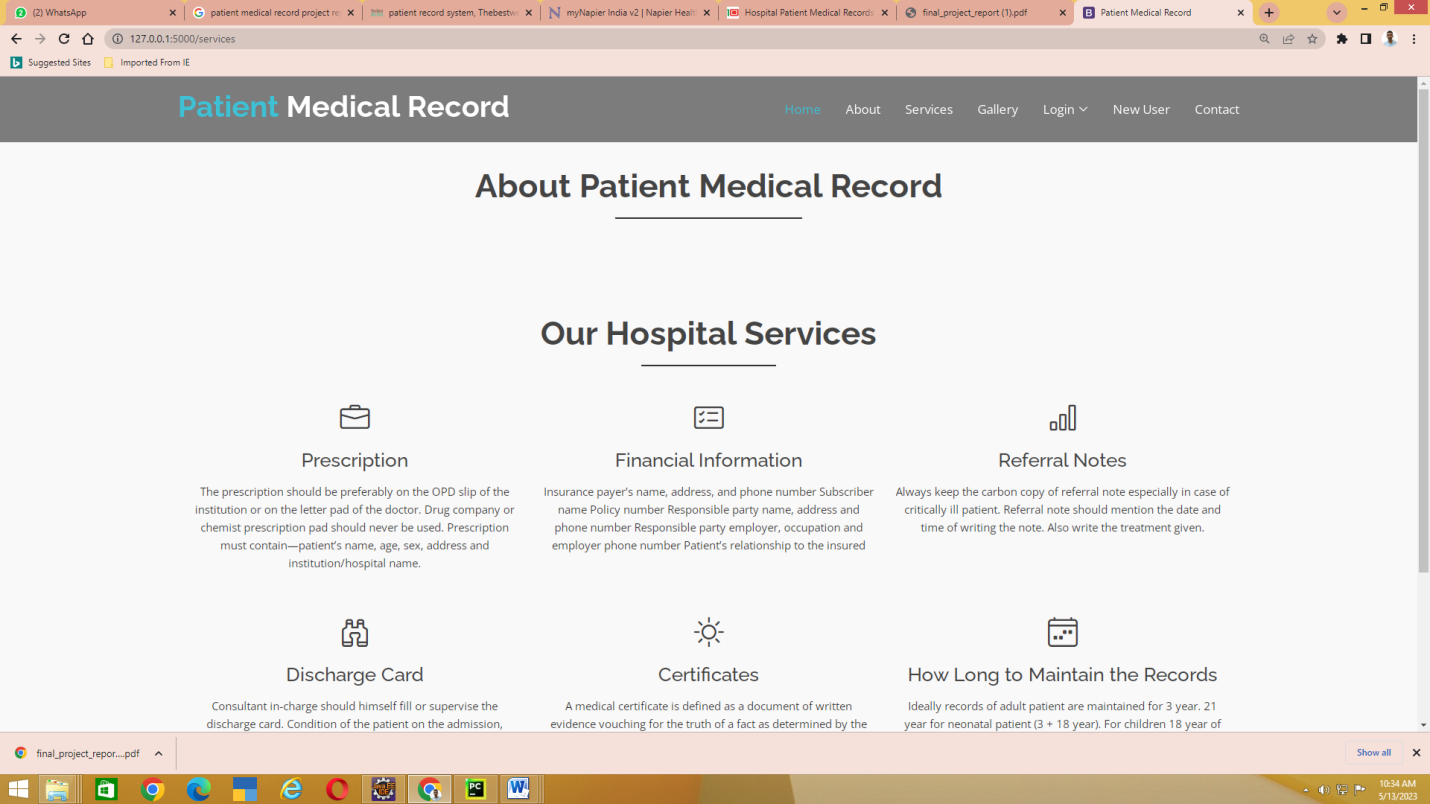
return str(e)

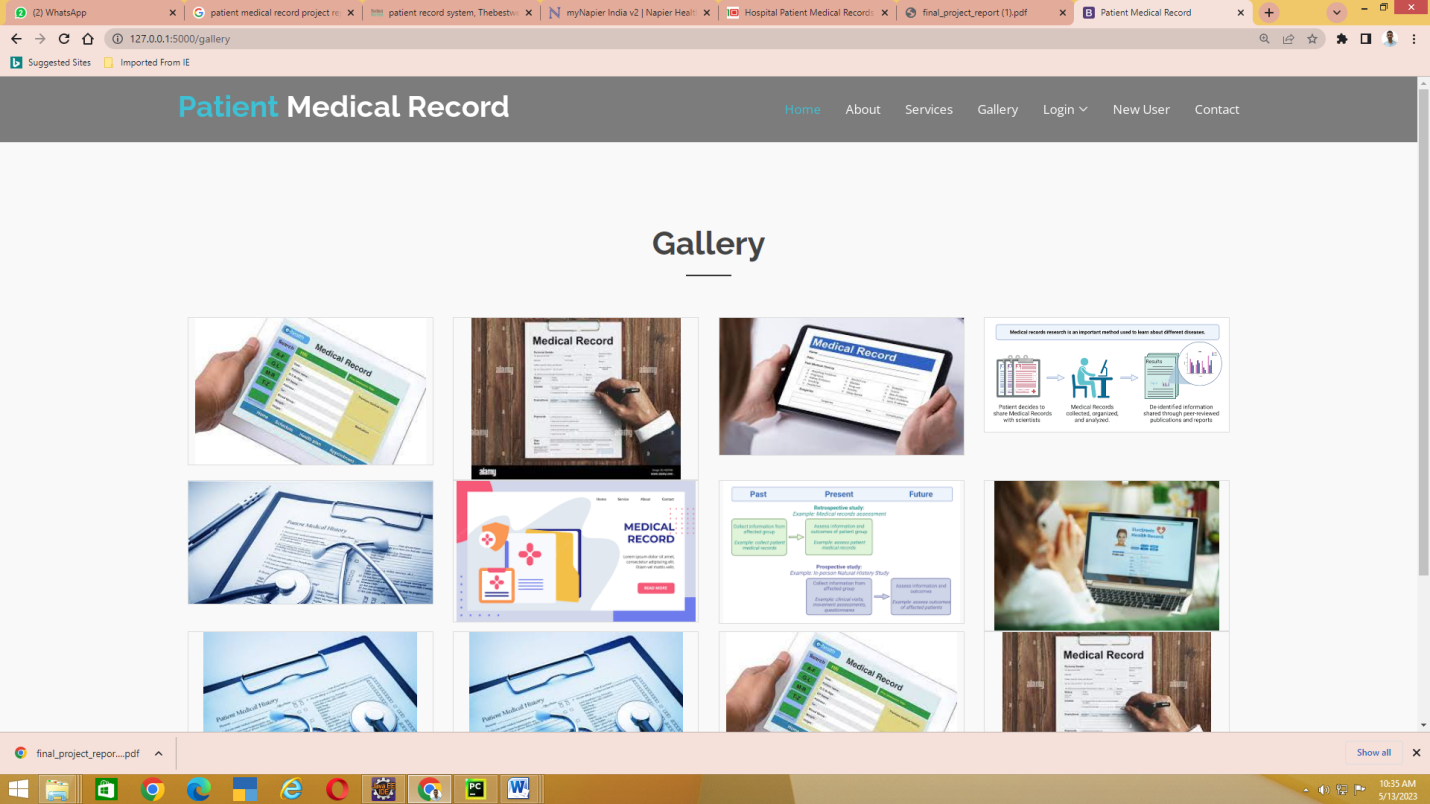
**APPENDIX-B**

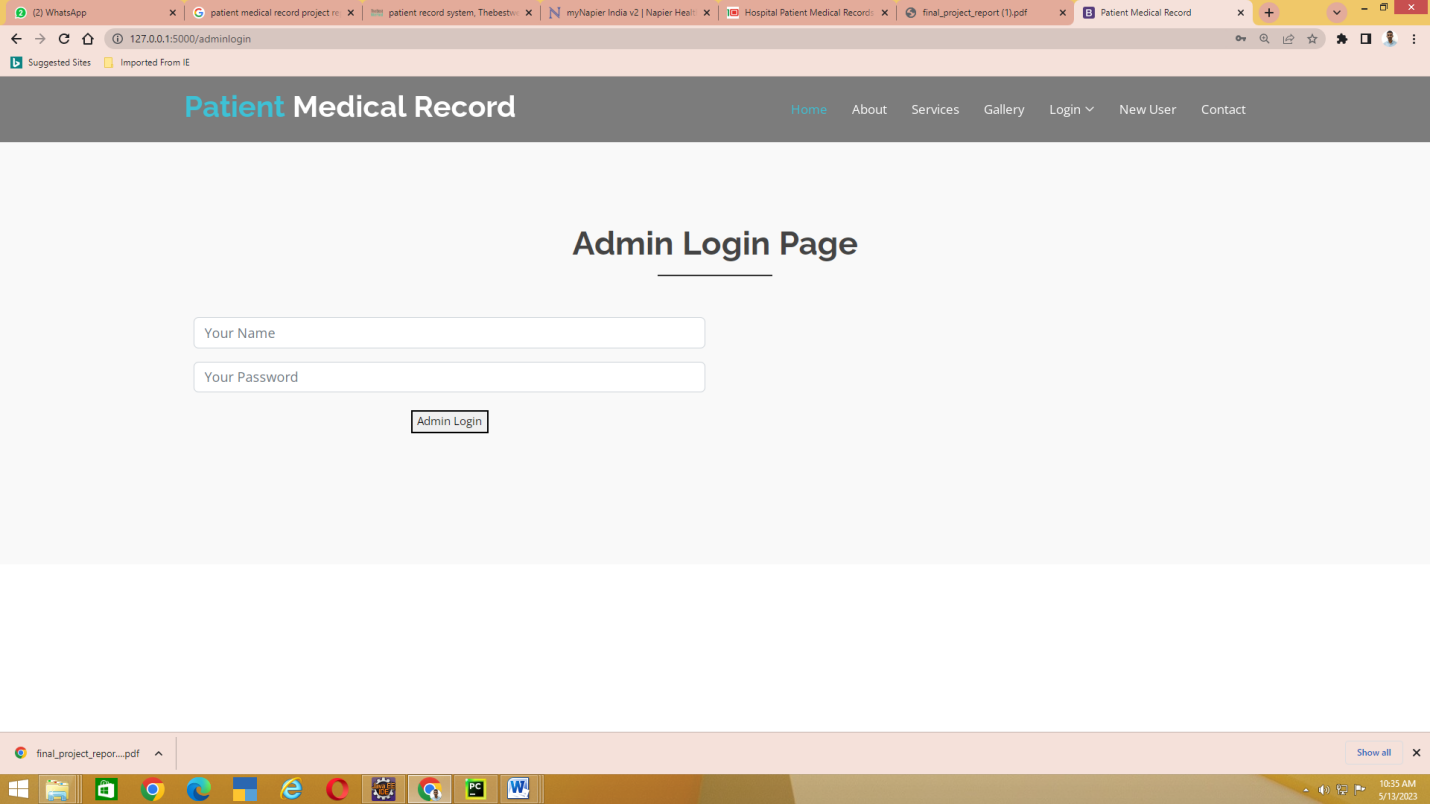
**SCREENSHOTS**

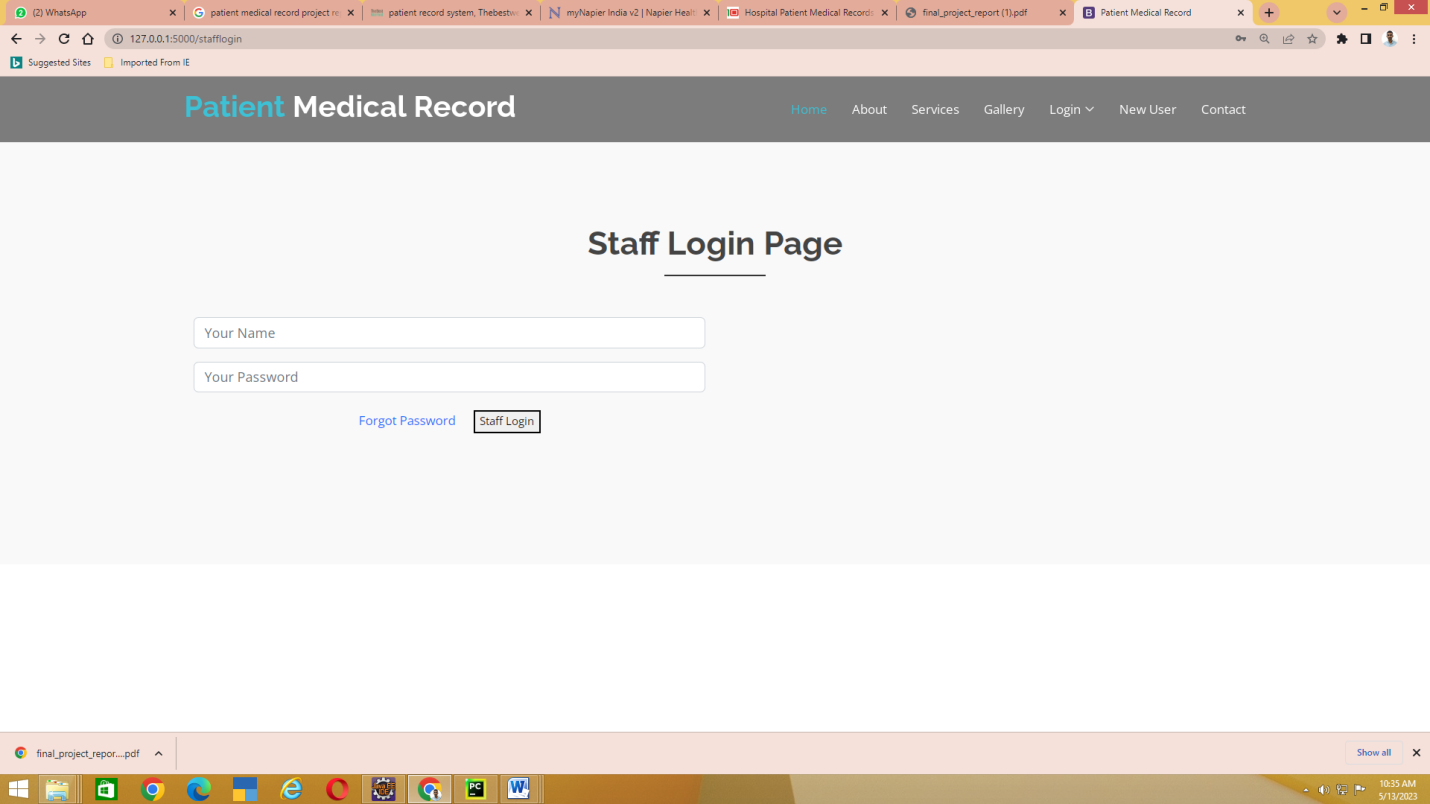


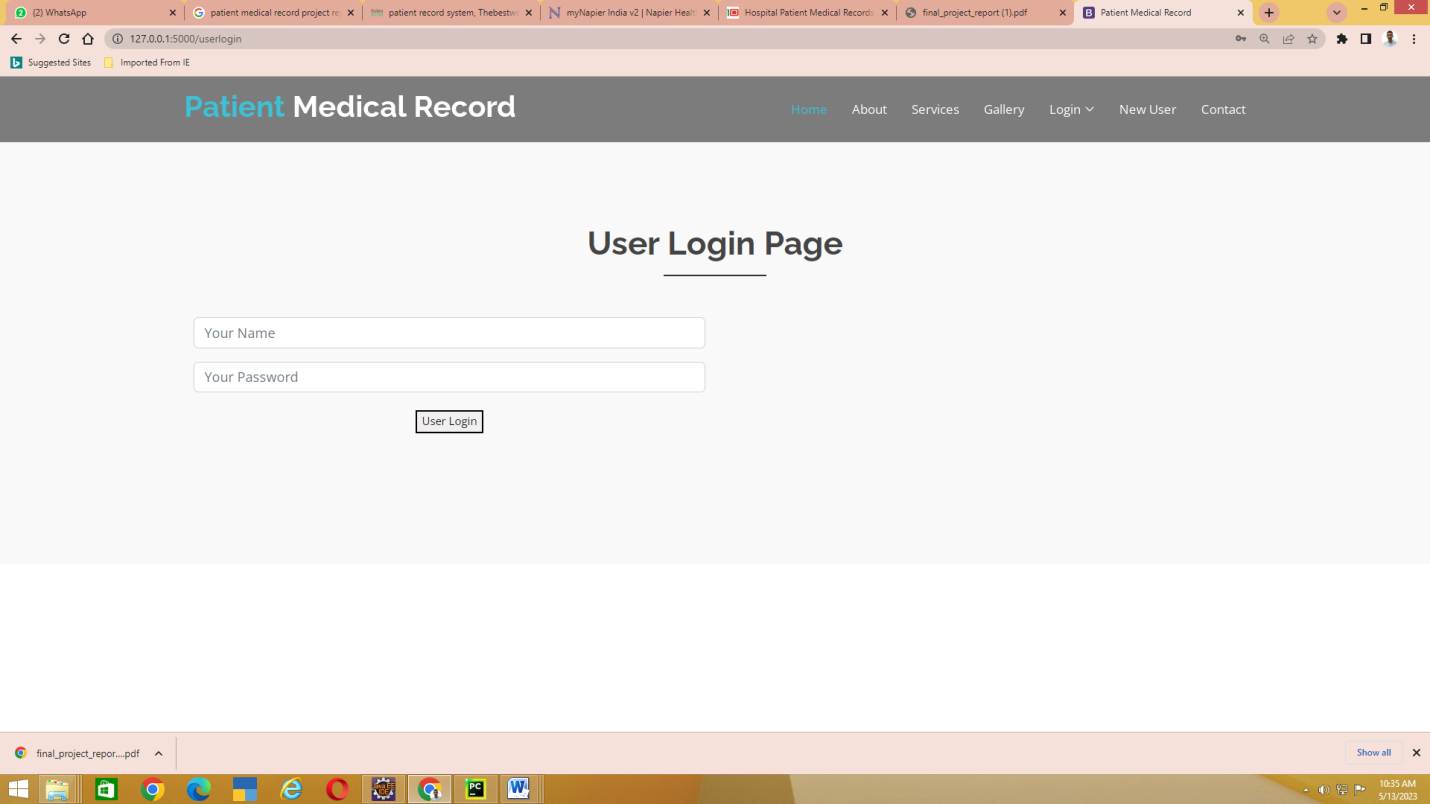


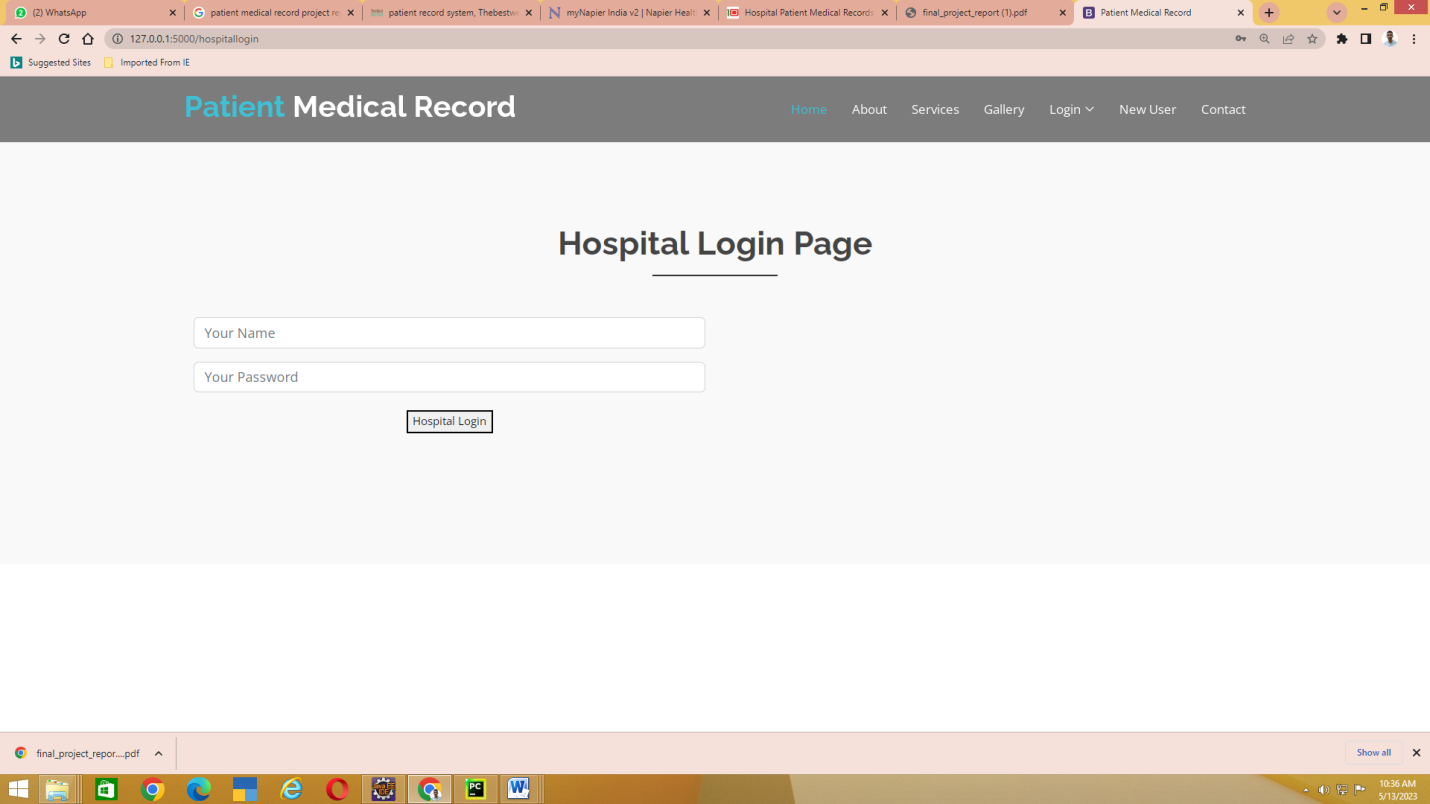


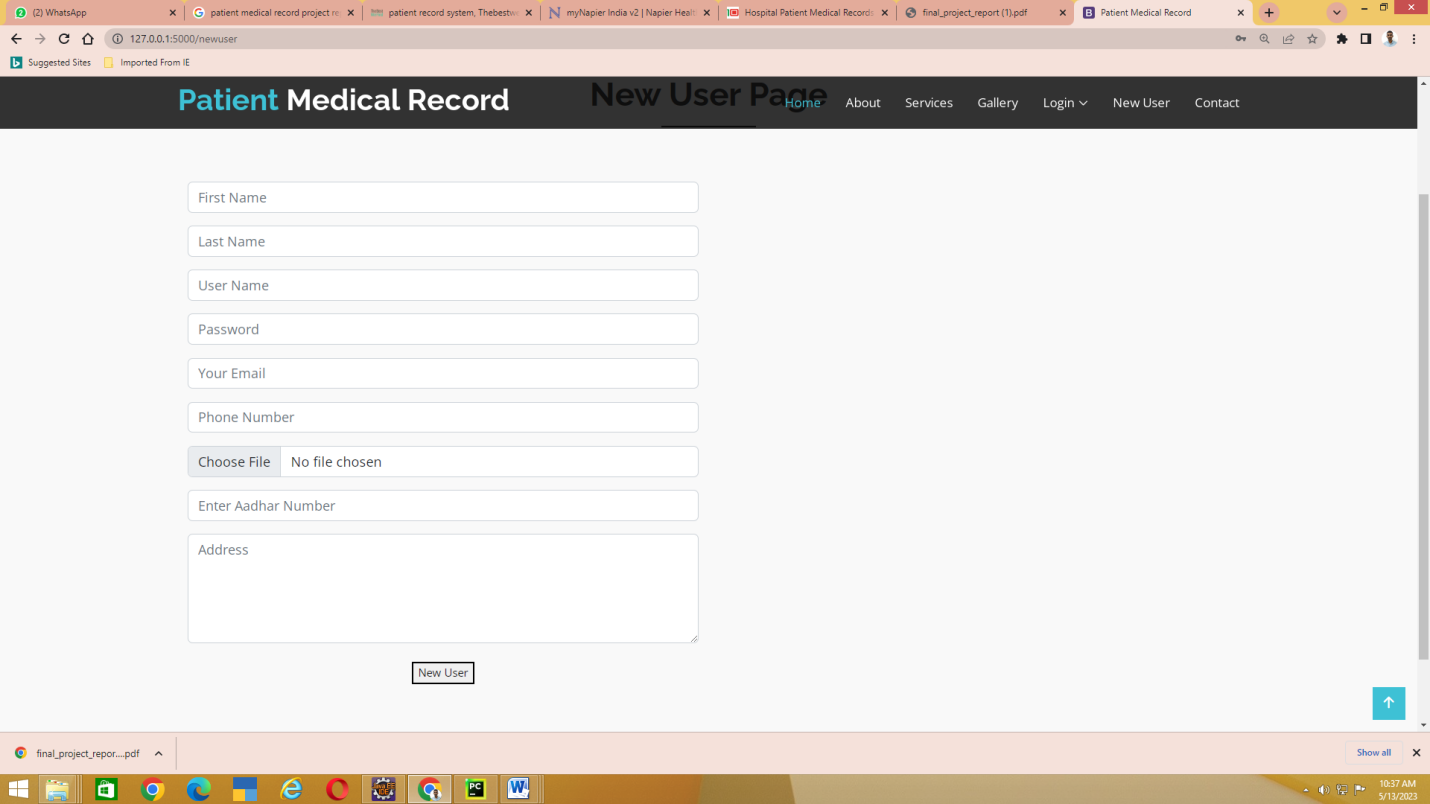


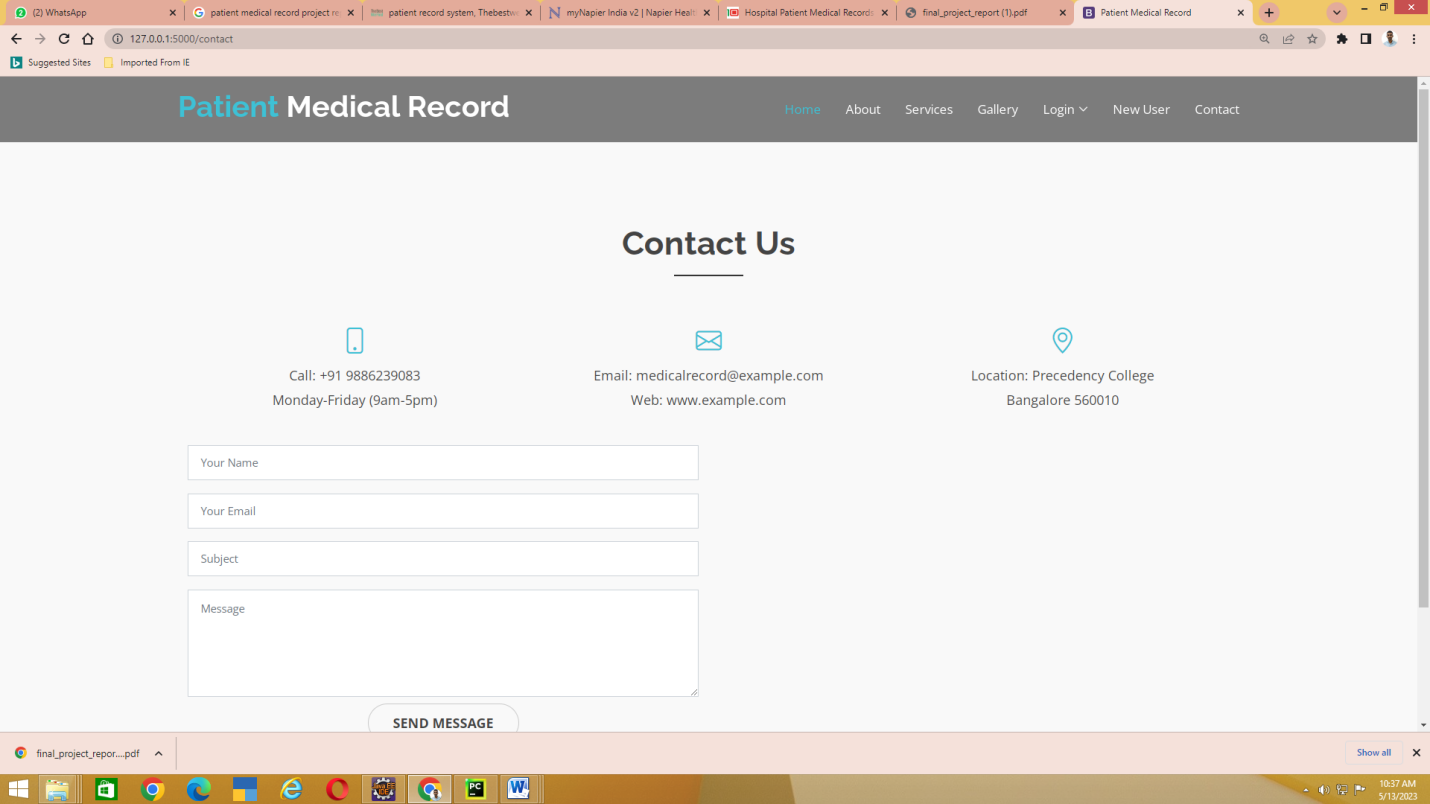


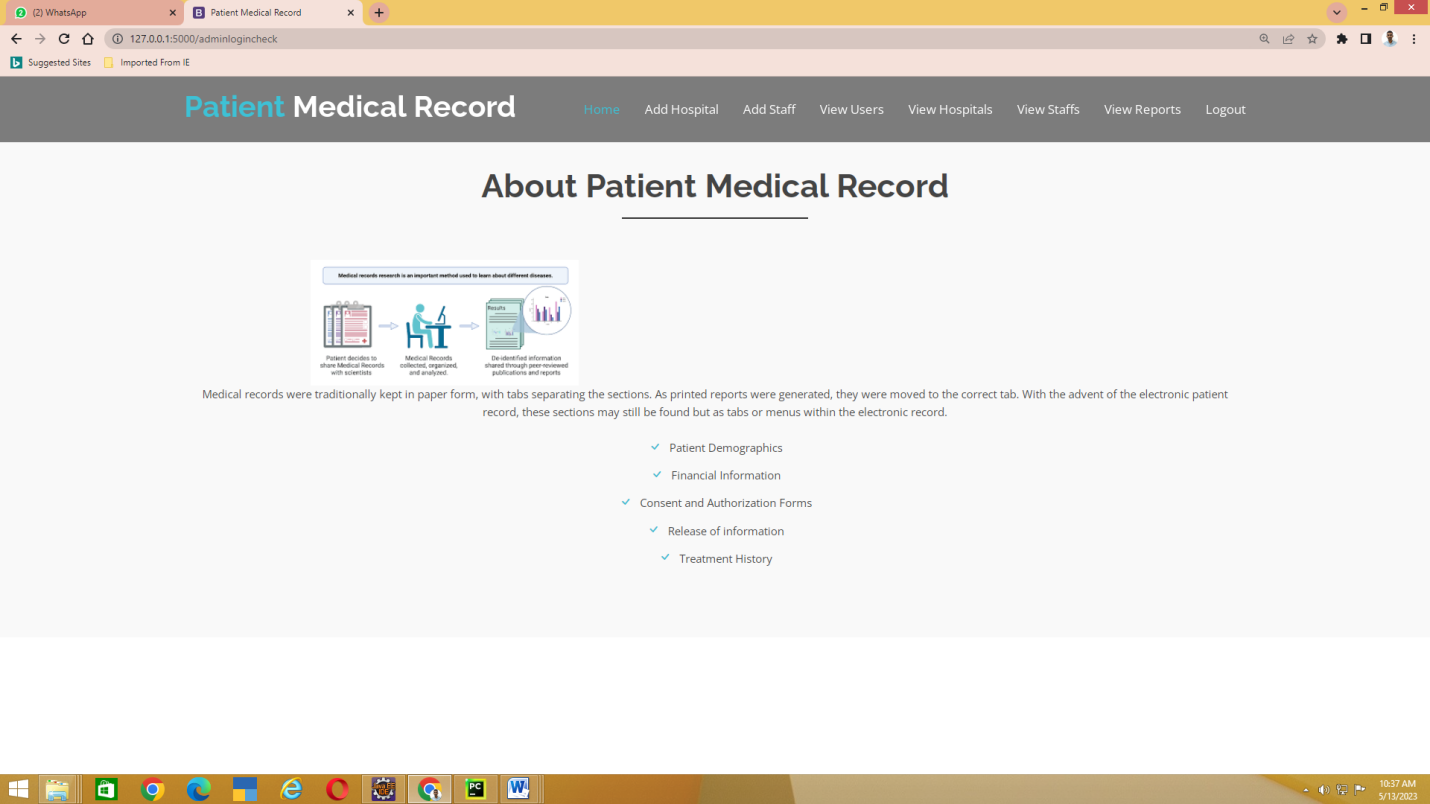


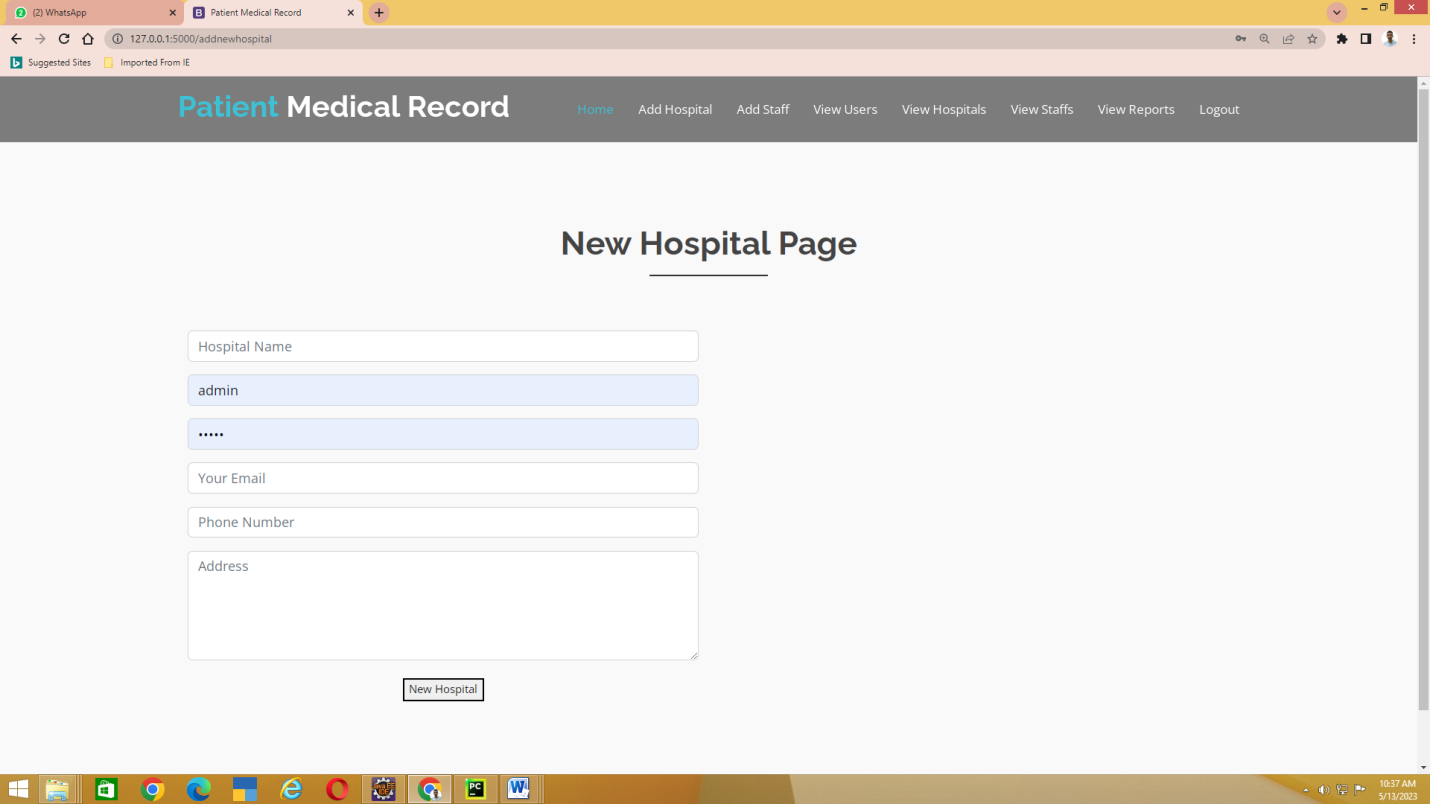


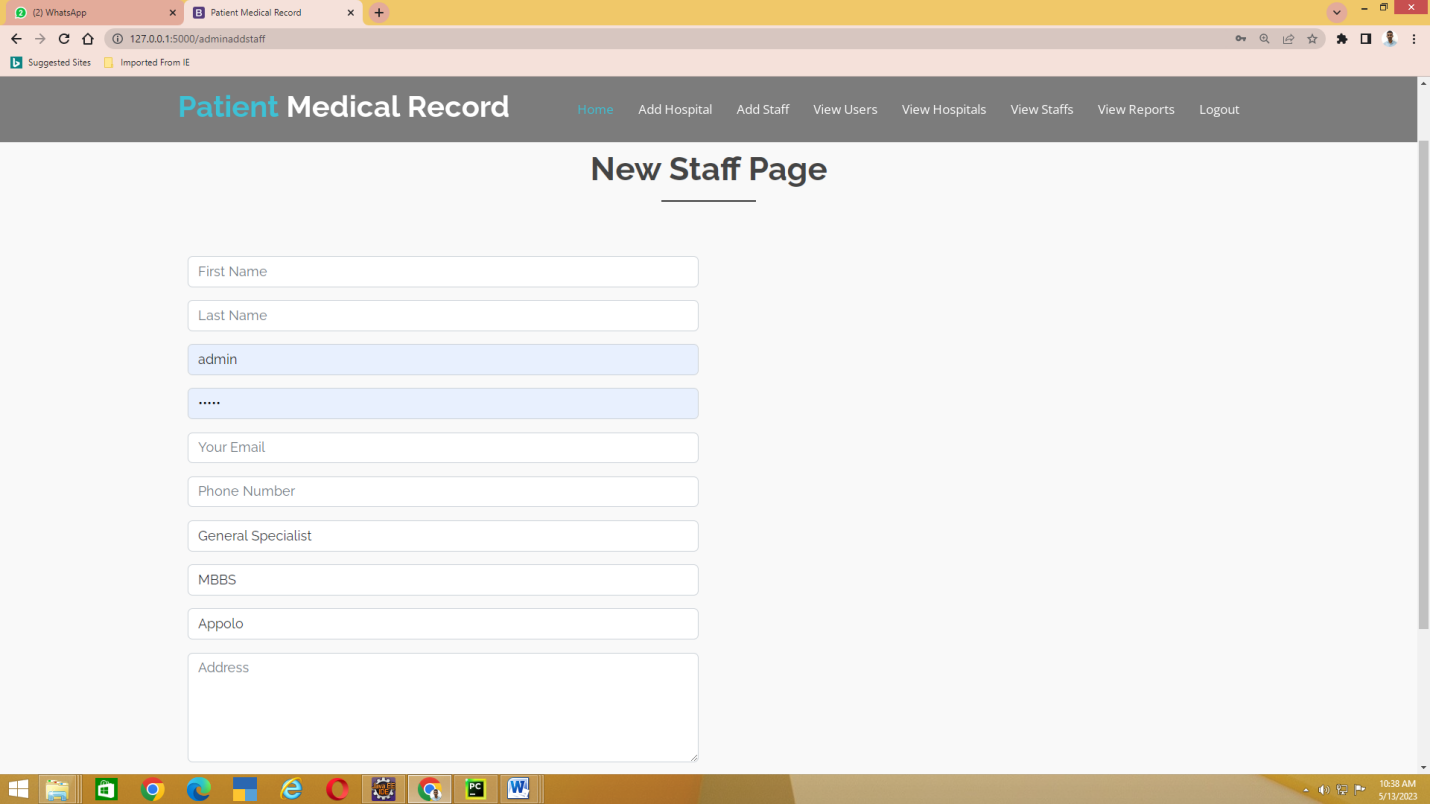








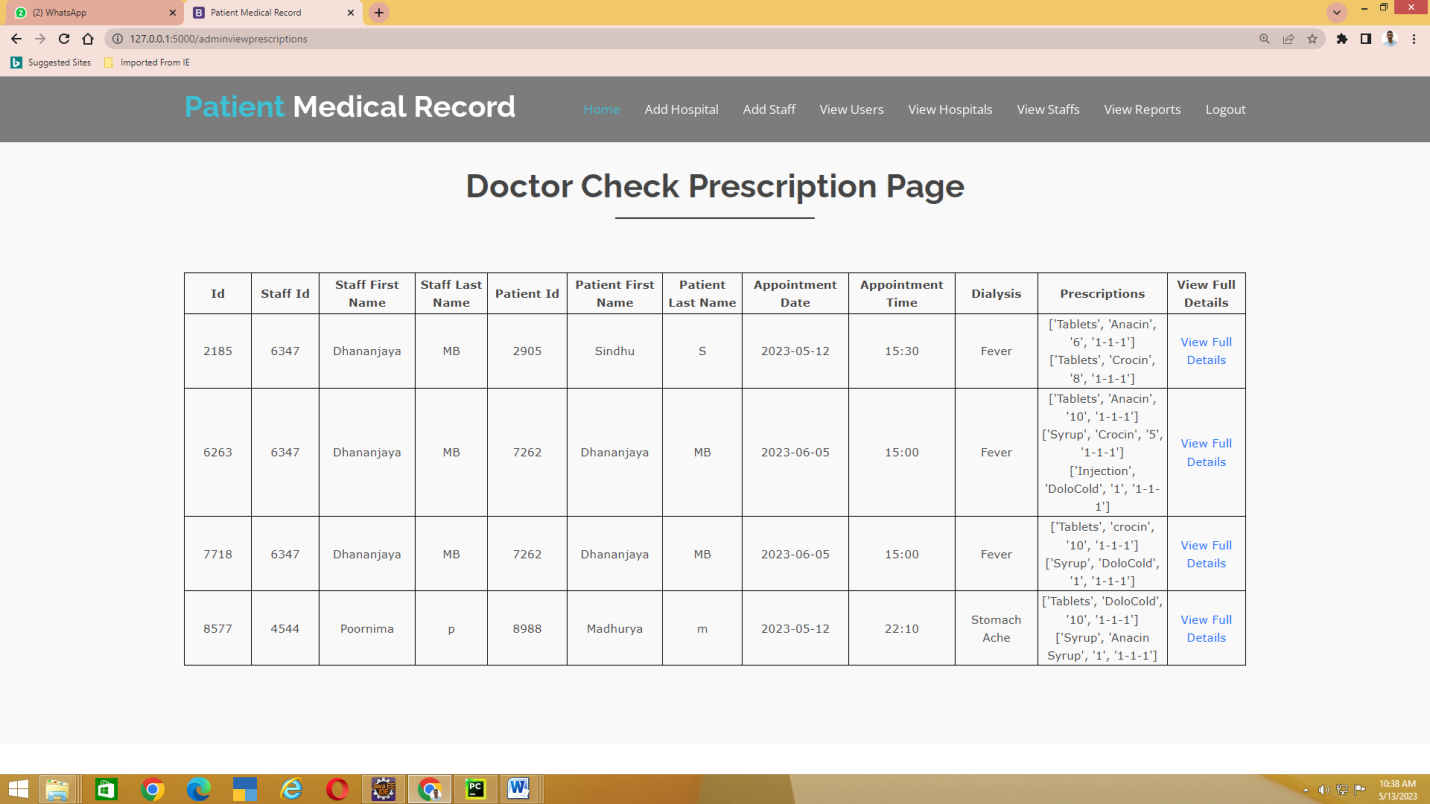












**APPENDIX-C**

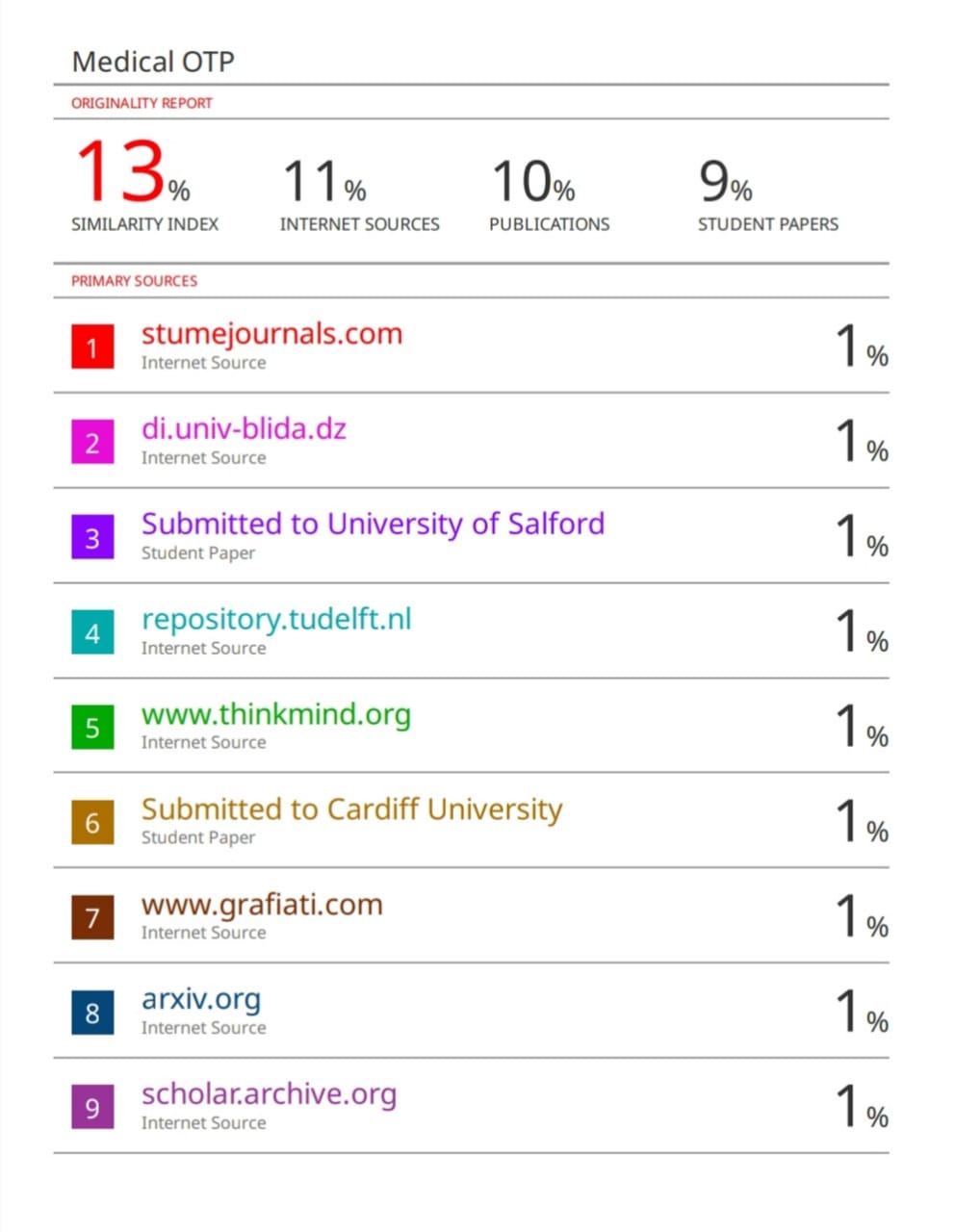
**ENCLOSURES**

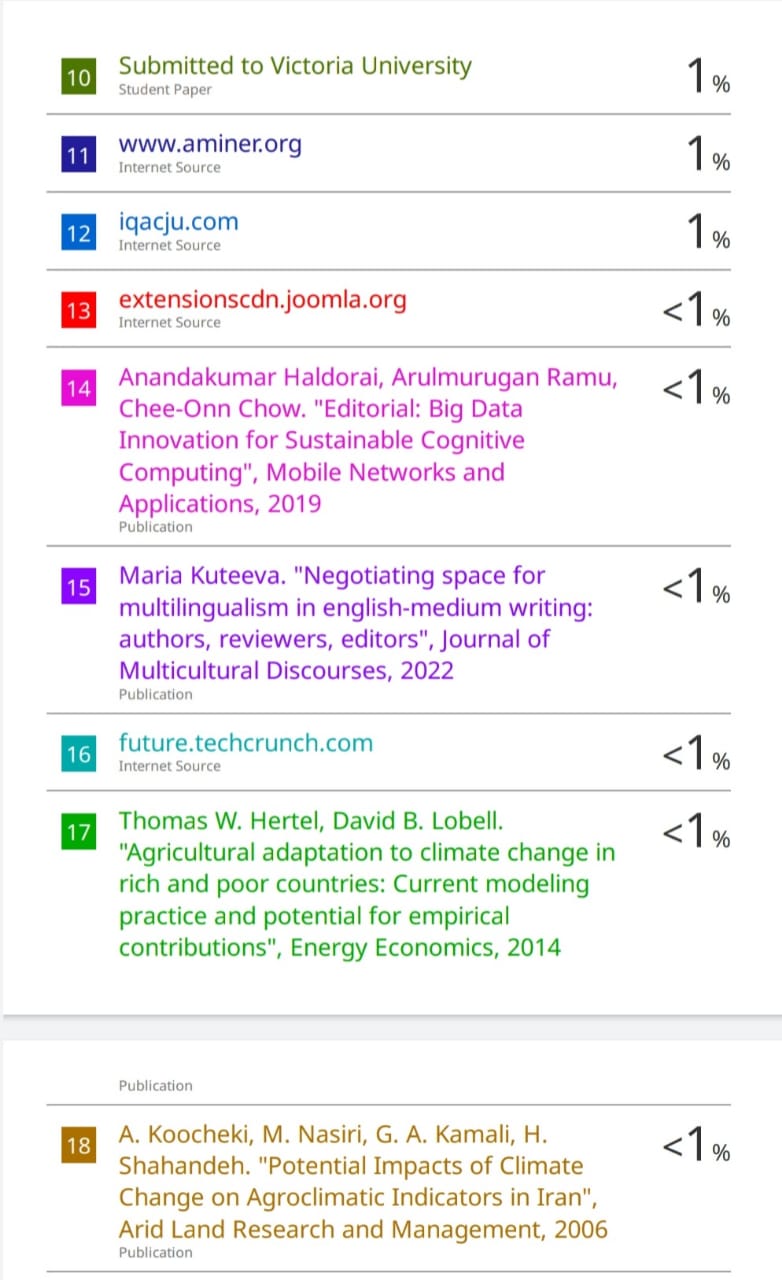
CERTIFICATE OF PUBLICATION

****

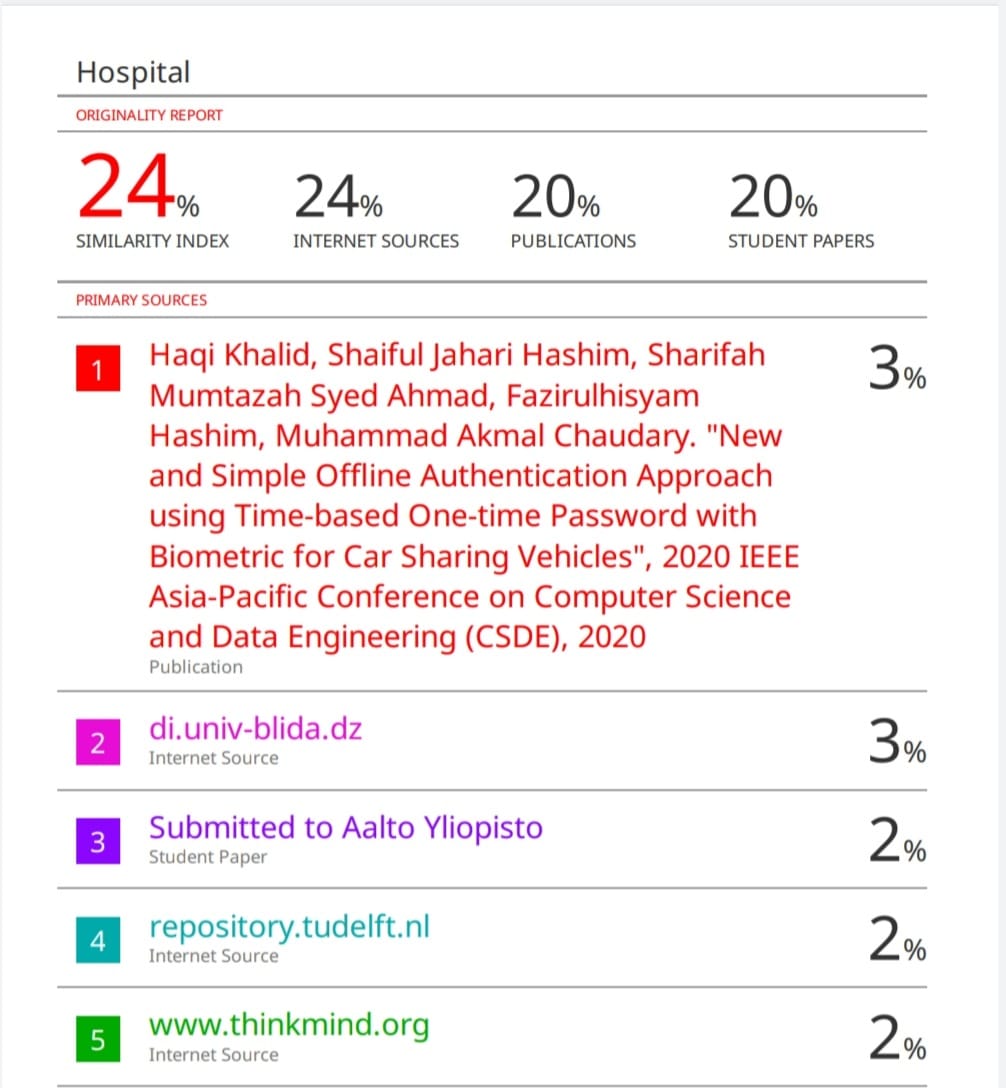
**PLAGIARISM**

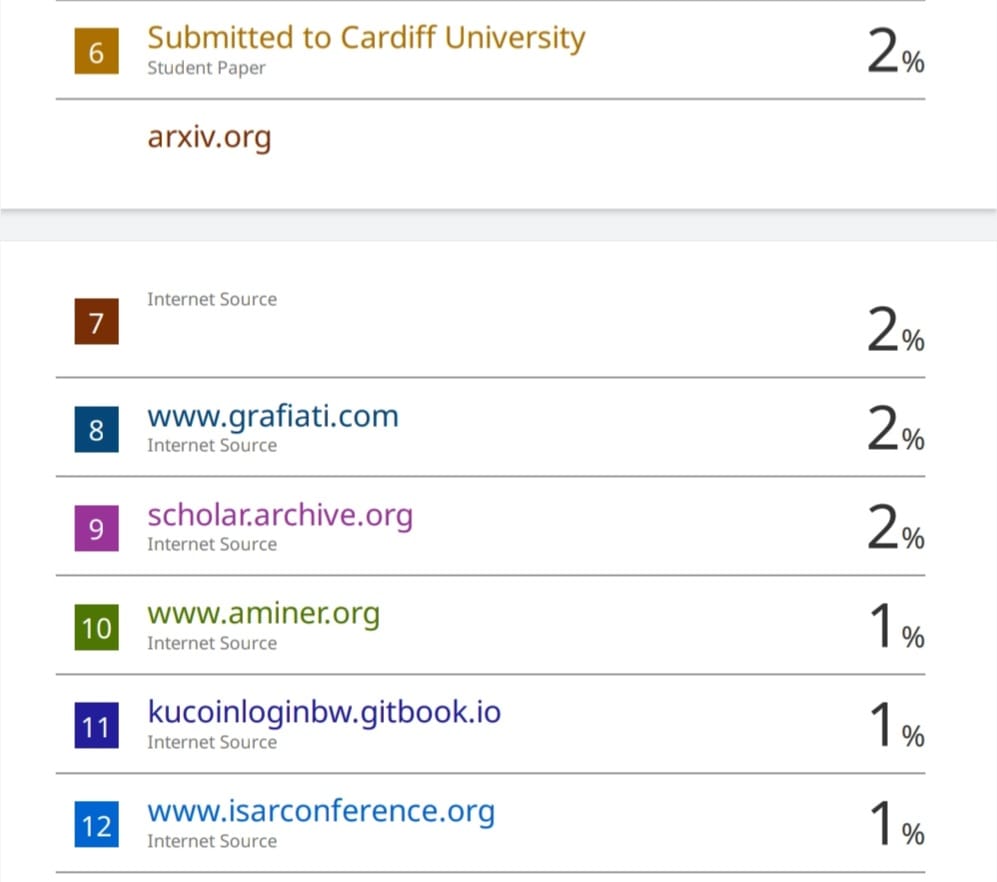
CONFERENCE PAPER PLAGIARISM

****

****

**REPORT PLAGIARISM**

****

****

**SUSTAINABLE DEVELOPMENT GOALS**

****

**The Project work carried here is mapped to SDG-3**

**Good health, well-being**

Ensuring good health and well-being is paramount in any hospital management system. The seamless integration of advanced technologies facilitates efficient patient care, from streamlined appointment scheduling to real-time monitoring of vital signs. Electronic Health Records (EHRs) enhance accuracy in diagnoses and treatment plans, fostering comprehensivehealthcaredelivery. Additionally, the system's data analytics capabilities enable proactive health management by identifying trends and potential outbreaks. Through telemedicine features, patients can access medical consultations remotely, promoting accessibility and reducing the burden on physical infrastructure. By prioritizing interoperability and security measures, a hospital management system contributes to a holistic approach in fostering good health and well-being within the healthcare ecosystem.