**CONFIDENTIALITY OF PATIENT MEDICAL RECORDS**

## A PROJECT REPORT

***Submitted by,***

**20201CSE0513 - Minal Saini**

**20201CSE0516 - Spoorthi B Kudagi**

**20201CSE0524 - Rohith PV**

### *Under the guidance of,*

**Dr. SHARMASTH VALI Y**

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

**BACHELOR OF TECHNOLOGY**

**IN**

**COMPUTER SCIENCE AND ENGINEERING**

**At**

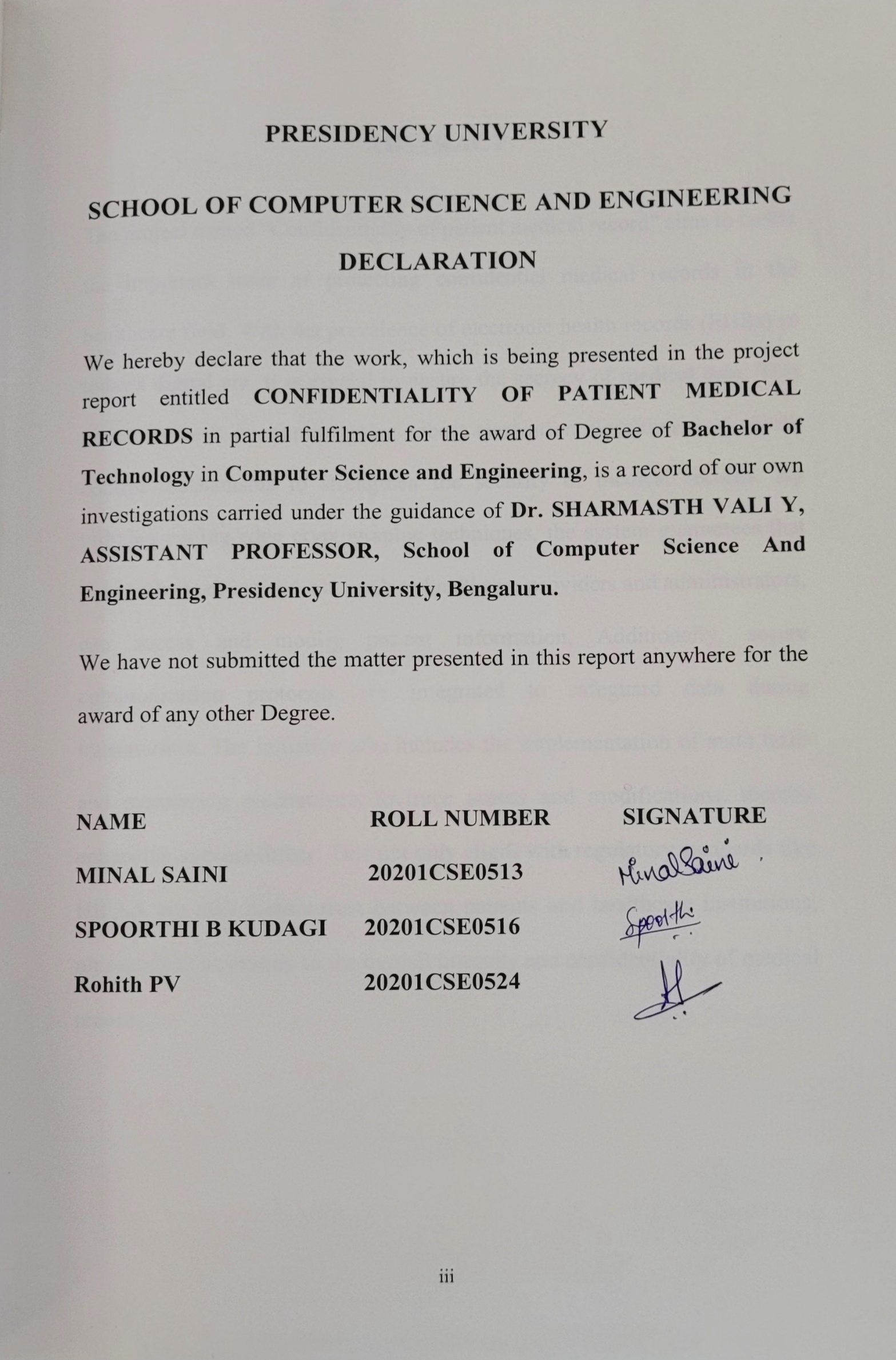


**PRESIDENCY UNIVERSITY**

**BENGALURU**

**JANUARY 2024**



****

|  |
| --- |
|  |

**ABSTRACT**

The project named “Confidentiality of patient medical record” aims to tackle the important issue of protecting confidential medical records in the healthcare field. With the prevalence of electronic health records (EHRs) in today's digital era, it is crucial to ensure the secrecy of medical data. This project focuses on implementing robust encryption algorithms and access control mechanisms to strengthen the security of medical records. By utilizing cutting-edge cryptographic techniques, the system guarantees that only authorized individuals, such as healthcare providers and administrators, can access and modify patient information. Additionally, secure communication protocols are integrated to safeguard data during transmission. The initiative also includes the implementation of audit trails and monitoring mechanisms to trace access and modifications, thereby enhancing accountability. This not only aligns with regulatory standards like HIPAA but also fosters trust between patients and healthcare institutions, ultimately contributing to the overall integrity and confidentiality of medical records.

**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 and 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 and Information Science, Presidency University and **Dr. Pallavi R**, Head of the Department, School of Computer Science and Engineering, Presidency University for rendering timely help for the successful completion of this project.

We are greatly indebted to our guide **Dr. Sharmasth Vali Y**, School of Computer Science and Engineering, Presidency University for his 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 **Mr Zia Ur Rahman, Mr. Penial John Whistley.**

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

**MINAL SAINI**

**SPOORTHI B KUDAGI**

**ROHITH PV**

**LIST OF TABLES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Table Name** | **Table Caption** | **Page No.** |
| 1 | 2.1 | Literature Survey | 5 |

**LIST OF FIGURES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No.** | **Figure Name** | **Caption** | **Page No.** |
| 1  2  3 | Figure 6.1.1  Figure 6.1.2  Figure 7.5 | Diagram explaining the verification  of user  Use Case diagram  Gnatt chart | 15  15  19 |

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | **ABSTRACT** | **iv** |
|  | **ACKNOWLEDGEMENT**  **LIST OF TABLES**  **LIST OF FIGURES** | **v**  **vi**  **vii** |
| **1** | **INTRODUCTION** | **1** |
| **2** | **LITERATURE SURVEY** | **5** |
| **3** | **RESEARCH GAPS OF EXISTING METHODS** | **8** |
| **4** | **PROPOSED METHODOLOGY**  4.1 Design steps  4.1.1 Project start-up  4.1.2 Requirement gathering and  Analysis  4.1.3 Backend programming  4.1.4 Creating user interface design  4.1.5 Frontend development with  material -UI and React  4.1.6 Integration and testing  4.1.7 Implementation | **11**  11  11  11  11  12  12  12  12 |
| **5**  **6** | **OBJECTIVES**  **SYSTEM DESIGN AND IMPLEMENTATION**  6.1 System Design  6.2 Implementation Details  6.2.1 To establish the project  6.2.2 Software Requirements  6.2.3 Hardware Requirements | **13**    **14**    14  16    16  16  16 |
| **7** | **Timeline for execution of project**  7.1 Review 0  7.2 Review 1  7.3 Review 2  7.4 Review 3  7.5 Final review | **18**  18  18  19  19  19 |
|  |  |  |
| **8** | **Outcomes** | **21** |
| **9** | **Results And Discussions** | **22** |
| **10** | **CONCLUSION** | **24** |
|  | **REFERENCES** | **25** |
|  | **APPENDIX-A**  **APPENDIX-B**  **APPENDIX-C** | **27**  **34**  **38** |

|  |  |  |
| --- | --- | --- |
|  |  |  |

**CHAPTER-1**

**INTRODUCTION**

Medical record confidentiality is an essential and basic component of healthcare that demonstrates a dedication to safeguarding patients' privacy and dignity. Ensuring the security of medical information is becoming more and more crucial as the healthcare industry changes due to developments in technology and shifting social expectations. With a focus on the historical foundations, ethical issues, legal frameworks, new problems, and technology solutions, this extensive six-page document seeks to offer a nuanced and in-depth exploration of the complex aspects of medical records confidentiality. We aim to highlight the vital role that secrecy plays in promoting trust, moral medical practice, and the provision of high-quality healthcare by carefully examining these factors.

The increasing prevalence and complexity of cyberattacks highlight how vital it is to protect medical records. Because of its vulnerability and potential for abuse, patient data is a highly sought-after target. Transgressions pertaining to confidentiality not only transgress moral norms but also undermine patient confidence in medical establishments. As a result, creative solutions that go above and beyond legal requirements to strengthen the privacy of medical records are desperately needed.

To fully appreciate the concepts that support medical record confidentiality's current significance, one must have a thorough understanding of the history of the practice. This section will examine the evolution of secrecy in medicine across time, following its origins from antiquated medical ethics—like the Hippocratic Oath—to the changing standards and procedures in contemporary healthcare.

We will examine significant turning points and moral frameworks that have influenced the idea of medical confidentiality, emphasizing the moral need to protect patient privacy across the ages.

The moral compass of healthcare is ethics, and the confidentiality of medical records is closely related to core ethical values. The ethical pillars of autonomy, beneficence, non-maleficence, and justice—all of which support the commitment confidentiality will be thoroughly covered in this section.

The project's diverse applications and ramifications go beyond data protection alone. Enhanced security measures add to the general credibility of healthcare organizations in addition to helping them comply with regulations. Collaborative patient care is facilitated by healthcare providers' confidence sharing of information through permitted channels. In turn, this strengthens the patient-doctor bond by giving patients more confidence that their private health information is handled with the highest secrecy.

In a time when data security is critical, this full-stack project essentially signifies a significant advancement in protecting the privacy of medical records. The project has the potential to reshape the requirements for reliable and safe healthcare information systems by resolving the drawbacks of earlier technologies and highlighting the value of secrecy.

The paper will examine the moral conundrums that medical personnel could run into when trying to strike a balance between the need to disclose information in order to improve patient care and the obligation to preserve patient privacy. Healthcare professionals might have a greater awareness of their duty to protect patient confidentiality by addressing these ethical issues.

The legal environment pertaining to the confidentiality of medical records is complicated and differs depending on the jurisdiction. A thorough study of important national and international laws, including the General Data Protection Regulation (GDPR) in Europe, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and other laws of a similar nature across the globe, will be provided in this part.

This section explores the legal rights and obligations of patient privacy with the goal of clarifying the legal frameworks that healthcare practitioners need to understand in order to maintain compliance and protect patient data.

The confidentiality of medical records is becoming more complicated and challenging as technology develops. The growth of electronic health records (EHRs), interoperability challenges, cybersecurity risks, and the effect of telemedicine on patient data security are some of the modern issues that will be examined in this section.

Healthcare workers must be aware of these issues in order to take proactive measures to close possible gaps in security and implement measures that improve medical record security in the digital era.

Technology also provides ways to strengthen medical record confidentiality in response to the changing environment. The technological developments that strengthen the security of patient information will be covered in detail in this part, including encryption, secure communication platforms, and artificial intelligence.

Further, the document will examine possible future paths for medical record confidentiality, taking into account best practices and innovations that could further improve data protection while maintaining accessibility for authorized healthcare providers.

As it wraps up this thorough investigation, the paper seeks to highlight how technological, ethical, legal, and historical aspects all play a connected role in protecting patient privacy. Healthcare practitioners who are committed to maintaining patient anonymity can effectively traverse the complicated landscape of modern healthcare by developing a comprehensive understanding of medical record confidentiality.

**CHAPTER-2**

**LITERATURE SURVEY**

**Table 2.1 Literature Survey**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | **Year** | **Authors** | **Advantages** | **Limitations** |
| Blockchain for Secure and Scalable Sharing of Healthcare Data | **2016** | 1. Azaria 2. Ekblaw 3. Vieira T 4. Lippma A | 1. Guarantees the confidentiality and inviolability of medical records. 2. Reduces the chance of a single point of failure, boosting security. 3. Offers a strong framework for security to prevent unwanted access. | 1. Need a large amount of processing power to implement consensus methods. 2. Scaling to support large healthcare systems has issues. |
| Privacy-preserving medical data sharing using homomorphic encryption | **2017** | 1. De Cristofaro 2. Faber, S. | 1. Allows computations on data that has been encrypted while maintaining privacy. 2. Facilitates secure outsourcing of calculations without revealing data. | 1. May need a lot of computation, which restricts utilization in settings with limited resources. 2. Algorithms employed may have impact on effectiveness. |
| Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data | **2006** | 1. Goyal, V 2. Pandey, O. 3. Sahai, A., | 1. Provides attribute-based, fine-grained access control. 2. Enhances data security. 3. Characteristics the requirement for intricate key management. | 1. Difficulty incorporating ABE into the current healthcare systems. 2. Scalability may be an issue. |
| Differential Privacy: A Survey of Results | **2008** | 1. Dwork, C. | 1. It offers a robust assurance of privacy. 2. Reduces the possibility that anonymized healthcare data will be the target of re-identification attacks. | 1. Might be difficult to find the ideal balance between data utility and privacy. 2. Differential privacy implementation may require a thorough understanding of the underlying mechanism. |
| A survey of secure multi-party computation protocols | **2014** | 1. Cascudo I. 2. Damgård I 3. RanellucciS. | 1. Enables group analysis without disclosing personal information 2. Encrypts data while it is being processed to protect against insider attacks. | 1. Resources-intensive nature might be problematic in settings when resources are few. 2. Can be difficult to guarantee compatibility between several secure computation protocols. |

1. Blockchain technology is starting to change how healthcare data is shared and secured. Blockchain protects the integrity of medical records by prohibiting unauthorized changes because it is decentralized and unchangeable. Stakeholders can securely monitor access and adjustments because to the transparent and traceable transactions included in a blockchain system, which also makes auditing easier. However, for successful integration into the healthcare ecosystem, obstacles like scalability and processing overhead must be resolved.
2. Leading the way in privacy-preserving technology is homomorphic encryption, which permits calculations on encrypted medical data without jeopardizing privacy. It makes it easier to securely outsource computations to outside services while guaranteeing that private information is secured throughout processing. While homomorphic encryption offers benefits in terms of safe outsourcing and fine-grained access control, it also adds computational complexity and might not be suitable for real-time processing settings.
3. In this paper, for healthcare records attribute-based encryption or ABE provides a versatile method of granular access control. There are still issues, nevertheless, such as the possibility of misconfiguration hazards, lack of support for dynamic modifications in access policies, and the requirement for conscious integration with the current healthcare systems.
4. Differential privacy techniques add controlled noise to statistical searches on medical records, thereby offering a strong privacy guarantee. By adjusting settings, this method strikes a compromise between privacy and data utility, accommodating different levels of privacy requirements. Although differential privacy reduces the danger of re-identification, its implementation is complicated by noise calibration and may not work well in situations with tiny datasets.
5. Without disclosing personal information Secure Multi-Party Computation (SMPC) facilitates cooperative healthcare analysis. It protects privacy in joint analyses and prevents insider threats by encrypting data while it’s being processed. The technology's dynamic cooperation features present viable answers for scenarios involving safe healthcare.

**CHAPTER-3**

**RESEARCH GAPS OF EXISTING METHODS**

For the purpose of developing the area and resolving current constraints, it is imperative to identify research gaps in the techniques currently used for the secrecy of medical information. The following are some areas of research that need more investigation:

**1. Implementation of Blockchain Presents Integration Challenges:**

While blockchain technology is frequently suggested for securing medical records, little thorough study has been done on the real-world difficulties and potential obstacles to integration with current healthcare systems. We should examine the unique organizational, interoperability, and technical difficulties involved with incorporating blockchain technology into various healthcare infrastructures. groups.

**2. Usability and Practical Application of Homomorphic Encryption:**

Although homomorphic encryption is a potent method, more study is required to address its usability issues and practical implementation hurdles in actual healthcare settings. We should examine scalability, computational effectiveness, and user experience issues when applying homomorphic encryption to massive medical record systems.

**3. Attribute-Based Encryption's (ABE) Acceptance and Usability:**

Although ABE provides fine-grained access control, little is known about its usability and user acceptance, particularly with regard to healthcare workers who deal with encrypted medical records. We should examine how healthcare professionals may successfully adopt and operate ABE-based access control systems by learning about the usability, user acceptance, and training needs decisions.

**4.Improving Sound Pressure Levels for Differential Privacy:**

Differential privacy includes noise to balance privacy and usefulness, however there is a need for study on optimizing noise levels for specific healthcare applications to guarantee the correct balance is reached. We should create frameworks or algorithms for dynamically varying noise

levels according to the characteristics of healthcare data and the particular privacy needs of various situations.

**5.Resource Optimization and Scalability in Secure Multi-Party Computation (SMPC):**

As The scalability and resource optimization of SMPC, particularly when it comes to large-scale healthcare datasets and collaborations, are not well studied despite the fact that it provides secure communication. A possible area of study would be how to make SMPC protocols for medical applications more scalable, less complex to compute, and with optimal communication overhead.

**6. Multidisciplinary Methods and Adherence to Regulations:**

Multidisciplinary studies that take into account legal, ethical, and human considerations are lacking since existing studies frequently concentrate on the technological components of secrecy. Furthermore, studies on maintaining adherence to changing healthcare laws are required. We should examine how technological solutions interact with ethical and legal issues, tackling difficulties while adhering to healthcare laws.

**7. Security Solutions Focused on the User:**

The human element is frequently overlooked in favor of technical solutions in research. The user-centric aspects of medical record security, including user behavior, awareness, and education, are not well understood. We should investigate methods for raising user consciousness, creating user-friendly security interfaces, and comprehending how human aspects affect the security posture in healthcare environments as a whole. disorders.

**8. Sturdiness and Adversarial Attacks on Security Protocols:**

Research on how resilient secrecy measures—like blockchain and encryption—are against adversarial assaults is lacking. Real-world application requires an understanding of potential vulnerabilities and the development of countermeasures. Investigating potential attack vectors for confidentiality technologies in the healthcare industry is important. This includes developing remedies for increased security and investigating adversarial machine learning approaches.

**9. Techniques for Preserving Privacy and Usability:**

It is common to ignore the practicality of privacy-preserving methods like safe multi-party computation and homomorphic encryption. Further investigation is required to comprehend the effects of these methods on healthcare professionals' user experiences and the usability of healthcare systems. It is recommended that usability studies be conducted to evaluate the effects of privacy-preserving measures on the workflows of healthcare practitioners. Additionally, solutions to improve user acceptance without sacrificing security should be investigated.

**10.Attribute-Based Encryption with Dynamic Access Control Policies:**

In attribute-based encryption, existing research frequently assumes static access control policies (ABE). However, research on effectively monitoring and updating access control policies dynamically is needed in dynamic healthcare systems. We ought to investigate the creation of dynamic access control policies in ABE that can adjust to shifting roles and responsibilities in the healthcare industry as well as changing needs for data exchange.

In an increasingly complicated healthcare environment, filling in these research gaps will help build more reliable, flexible, and approachable solutions for maintaining the privacy of medical records.

**CHAPTER-4**

**PROPOSED METHODOLOGY**

**4.1 DESIGN STEPS:**

A suggested approach for creating a medical record management system with Express.js, Node.js, MongoDB, JWT token authentication, and Material-UI with React on the front end is given below. The processes from project commencement to deployment are outlined in the methodology:

**4.1.1 Project Start-Up:**

* Identify key stakeholders, such as administrators, possible system users, and healthcare professionals.
* Define the scope of the medical record management system, including features and user responsibilities.

**4.1.2** **Requirements Gathering and Analysis:**

* Understand and describe the functional and non-functional requirements of the system.
* Identify data entities, relationships, and access control requirements for medical records. Provide use cases and user stories for the CRUD (Create, Read, Update, Delete) actions on medical records.

**4.1.3 Backend** **Programming (Node.js and Express.js):**

* Put into practice the server-side logic for managing health records. Configure the Express.js program to respond to HTTP requests.
* Establish controllers and routes for CRUD tasks on medical records.
* MongoDB integration is needed to store and retrieve medical records.
* Implement authentication middleware using JWT tokens.

**4.1.4 Creating User Interface Design:**

* Creating a user-friendly and intuitive interface that facilitates successful communication between healthcare practitioners and patients and the system.
* Through the creation of the chat, sign-up, login, and user pages. These are the user interface photos.

**4.1.5** **Front-end development with Material-UI and React:**

* Create a frontend that is responsive and easy to use for dealing with medical records.
* Use Create React App to set up a React application.
* Integrate backend API calls for the creation, editing, deletion, and presentation of medical records.
* Use JWT tokens to implement user permission and authentication.

**4.1.6 Integration and Testing:**

* Use tools like Postman to test API endpoints for CRUD activities. Ensure that the frontend and backend components integrate seamlessly.
* Conduct integration testing to check the communication between frontend and backend.

**4.1.7 Implementation:**

* Release the medical record management system into a production environment.
* Install backend (Express.js and Node.js) and frontend (React) applications.
* Make the system available for use in production.

**CHAPTER-5**

**OBJECTIVES**

The Key aims and outcomes are addressed by the objectives of the proposed medical record management system project. The project's goal is to improve medical records' usability, accessibility, and confidentiality by utilizing best practices and contemporary technologies. The main goals are listed below:

**Confidentiality and Security:** Put strong security measures in place to guarantee the privacy and accuracy of medical records. In healthcare systems, patient information security is critical. In order to provide a secure and private environment for medical records, the project will use technologies such as JWT token for authentication and encryption for data security.

**User-Friendly Interface:** Provide administrators and healthcare professionals with an intuitive and user-friendly interface. -The usability of the technology is critical to its acceptance and success. React and Material-UI are used to create a frontend that is responsive and aesthetically pleasing, improving the user experience in general.

**Interoperability and Integration:** To Ensure interoperability and seamless integration with existing healthcare systems. Healthcare environments generally have varied systems and technologies. With seamless integration with current infrastructures, the project hopes to create a coherent and interoperable healthcare environment.

**User acceptability and Satisfaction:** Attain high levels of user acceptability and satisfaction among administrators and healthcare professionals. The project's ability to succeed hinges on user acceptance. In order to improve the system according to user preferences and demands, user acceptability testing and ongoing feedback mechanisms are put into place.

All of these goals work together to build a medical record management system that is safe, effective, and easy to use, meets industry standards, and improves patient care overall.

**CHAPTER-6**

**SYSTEM DESIGN & IMPLEMENTATION**

**6.1 SYSTEM DESIGN**

System design forms the backbone of any successful application or system. It serves as a **blueprint**, meticulously outlining the various components, workflows, tasks, and user interactions that bring the system to life. This crucial phase translates abstract ideas into concrete plans, ensuring every aspect is well-defined and seamlessly integrated.

By encompassing both functional and technical considerations, system design provides a **holistic view** of how the system will be implemented. It delves into the system's architecture, data structures, algorithms, and interfaces.

This in-depth exploration allows developers to grasp the complexities involved and make informed decisions throughout the development journey.

One key benefit of system design is its ability to **optimize resource allocation**. With a clear roadmap, developers can prioritize tasks and allocate resources strategically. This prioritization ensures focus on crucial components and functionalities, leading to a **more efficient and streamlined development process**.

Furthermore, system design marks the pivotal point where concept translates into reality. It bridges the gap between ideation and implementation, offering a **tangible plan** to guide developers. This phase empowers them to make informed decisions, anticipate potential challenges, and proactively develop solutions.

In essence, system design is an **irreplaceable step** in the development process. It provides a comprehensive roadmap, fosters efficient resource management, and facilitates a smooth transition from concept to creation.

Ultimately, it paves the way for a successful implementation, transforming abstract ideas into functional and impactful applications.

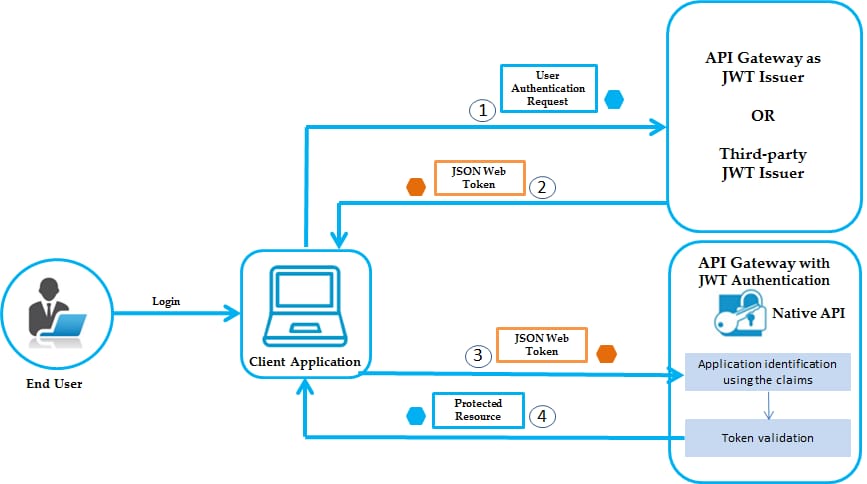


Figure 6.1.1 Diagram explaining the verification of user

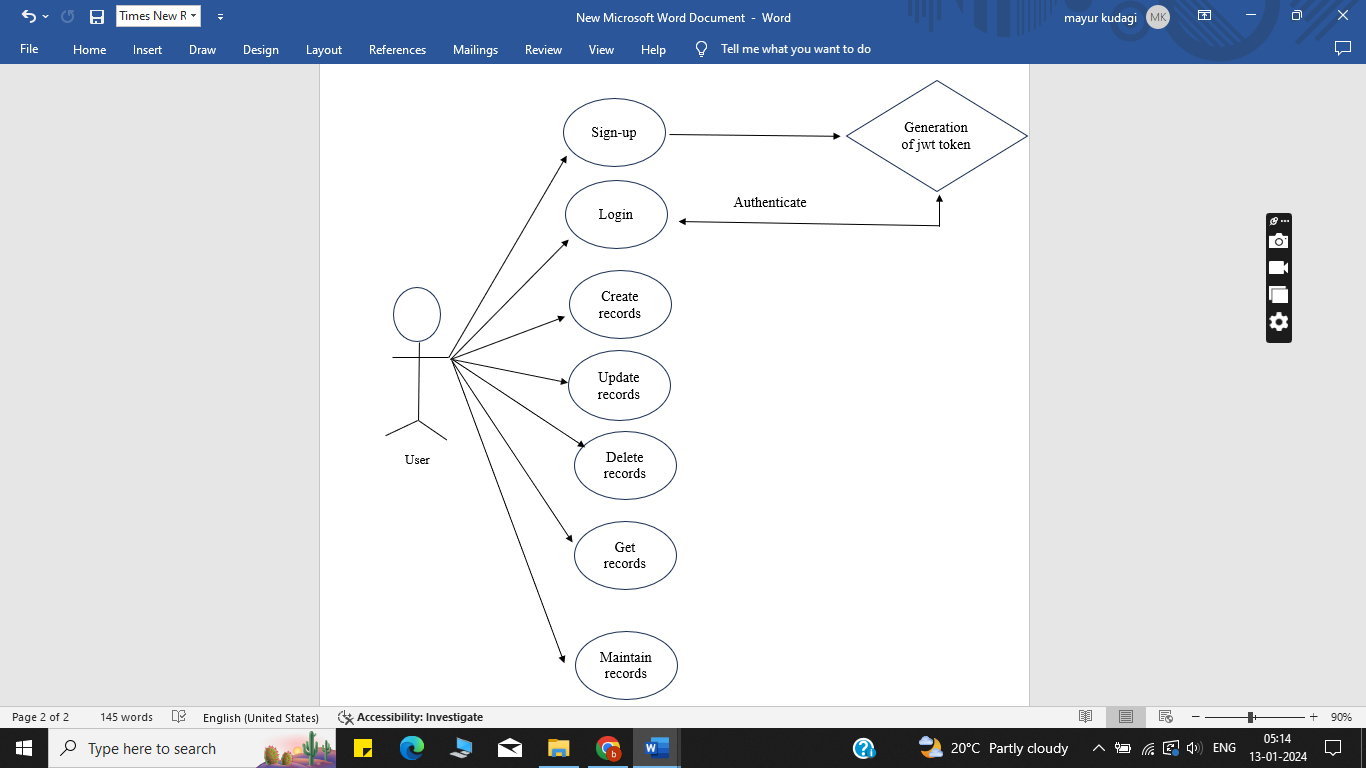


Figure 6.1.2 Use Case Diagram

**6.2** **IMPLEMENTATION DETAILS**

**6.2.1 To establish the project:**

* Start a fresh Node.js project by utilizing a package management such as npm.
* Install essential dependencies, including Express.js, Mongoose for MongoDB, and json web token for JWT token handling.
* Establish a server:

To process HTTP requests, set up a server using Express.js. Define the pathways for system administration, CRUD operations on medical records, and authentication.

* Establish a MongoDB connection:

Using Mongoose, create a connection to the MongoDB database. Provide database models that account for users, medical records, and other pertinent things.

* Put Authentication Middleware in Place:

Create middleware that uses JWT tokens to authenticate users. Make sure that access to protected routes is restricted to authorized users only.

* Security Procedures:

Use extra security precautions, like secure password processing, input validation, and HTTPS for encrypted communication.

**6.2.2 Software Requirements:**

* Programming Languages: JavaScript
* Library: Node Js
* Framework: express js
* library : React

**6.2.3 Hardware Requirements:**

* Windows 10, 64-bit OS
* 8Gb Ram and 512 SSD
* Intel i5 processor

**CHAPTER-7**

**TIMELINE FOR EXECUTION OF PROJECT**

**(GANTT CHART)**

* 1. **Review 0**
  + **Title Finalization with Supervisor**: Meet with your project supervisor to discuss and finalize the project's title. This step ensures that you and your supervisor are aligned on the project's focus.
  + **Literature Survey**: Start researching relevant literature in your field. This involves reading academic papers, articles, and books related to your topic. The literature survey helps you understand the existing research in the area.
  + **Finalizing Objectives**: Define the specific objectives and goals of your project. What do you aim to achieve? What problems are you trying to solve?
  + **Deciding the Methodology**: Determine the research methodology you'll use in your project, whether it's experimental, survey-based, analytical, or a combination of methods.

**7.2. Review 1**

* + **Title**: After finalizing with your supervisor, formally decide on and document the project title.
  + **Abstract:** Write the project abstract, a concise summary of your project's purpose, methodology, and expected outcomes.
  + **Literature Survey**: Continue your literature survey and ensure that you've referred to at least one research paper in your work.
  + **Identify**: The advantages and the disadvantages of our project.
  + **Software and Framework Details**: List the software framework tools or platforms you plan to use.
  + **References**: Site all the sources you've used in your literature survey.

**7.3 Review 2**

* + **Source Code Details:** Document your source code, including explanations and comments.
  + **50% Implementation Details with Live Demo:** Implement at least half of your project and present a live demonstration.
  + **50% Report Softcopy:** Submit a softcopy of the project report with 50% completion.

**7.4 Review 3**

* + **Source Code Details**: Continue documenting and explaining your source code.
  + **50% Implementation Details with Live Demo**: Complete 75% of the project implementation and demonstrate it live.
  + **75% Report Softcopy**: Submit a softcopy of the project report with 75% completion.
  + **75% Report Softcopy**: Submit an updated softcopy of the project report with 75% of the content.

**7.5 Final Review**

* + **Final Report and Submission of Project**: Complete your project, finalize the report, and submit the final project and report to your supervisor or institution.
  + Complete implementation details with live demo.
  + Submitting the final report to the reviewer.

Figure 7.5 Gnatt Chart

**CHAPTER-8**

**OUTCOMES**

It is anticipated that the medical record management system's effective deployment will have a number of beneficial effects that will improve patient care overall and the healthcare environment. Some major results that are expected from the project are listed below:

**1. Better Data Security:** As a result of the project's implementation, security measures to safeguard the integrity and confidentiality of medical records will be strengthened.

**2. Access Control:** To prevent unauthorized access to medical records, the project may involve putting access control systems in place.

**3. Effective Management of Medical Records:** Healthcare personnel may effectively manage medical records thanks to the system's CRUD (Create, Read, Update, Delete) functions. Processes are streamlined, there is less paperwork, and patient information is accessible more quickly as a result.

**4. Easy-to-use Interface for Medical Practitioners:** Healthcare workers will be able to explore and interact with the system with ease thanks to the development of a user-friendly interface made possible by React and Material-UI. Increased customer satisfaction and adoption result from this.

**5. Sophisticated System Management:** With specialized interfaces, system administrators may effectively manage user roles, permissions, and configurations. This makes it possible for the medical record management system to be administered smoothly.

**6. Optimization of Resources:** Improved coordination and insight into patient data and scheduling can lead to the efficient use of resources, such as medical personnel, facilities, and equipment.

**7. Patient Outcome Improvements:** With easier access to accurate and up-to-date medical information, healthcare professionals can make more informed decisions, leading to improved patient outcomes and a higher standard of care.

**CHAPTER-9**

**RESULTS AND DISCUSSIONS**

In addition to improving healthcare services and safeguarding patient privacy, a project that attempts to maintain the confidentiality of medical records serves other important reasons. The following are some main points emphasizing the value and application of this kind of project:

* **Protection of Patient Privacy:** An essential component of healthcare ethics is confidentiality. Putting in place a method to preserve medical records guarantees that private patient data is shielded from unwanted access, fostering patient-provider confidence.
* **Observance of Regulations:** Several data protection and privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) in the US, apply to the healthcare sector. Healthcare organizations can ensure ethical data handling methods and prevent legal ramifications by focusing on confidentiality projects that help them comply with these regulations.
* **Reduced Risk of Identity Theft:** Personal identifiable information (PII) is frequently included in patient records. By preventing the exploitation of private information like names, addresses, and social security numbers, medical record confidentiality reduces the danger of identity theft.
* **Enabling Reputable Healthcare Providers:** When patients have confidence that their private information will be kept private, they are more inclined to seek and follow medical advice. Better healthcare outcomes are a result of this, as it strengthens the doctor-patient bond.
* **Safe Data Exchange and Cooperation:** When The project should enable secure data sharing among authorized healthcare providers while respecting

confidentiality. By guaranteeing that individuals participating in a patient's treatment have access to pertinent information, this encourages collaboration in patient care.

* **Decrease in Medical Errors:** Medical errors can be decreased with the help of a private medical record system. Equipped with comprehensive and precise data, healthcare professionals may make well-informed choices that enhance patient safety and care quality.
* **Effective Provision of Healthcare:** Healthcare workers can obtain patient data more quickly and efficiently by minimizing the time they spend on administrative duties when they have access to a private, secure medical record system.

**CHAPTER-10**

**CONCLUSION**

In summary, maintaining the privacy of medical information is not just required by law; it is also a basic commitment to the three guiding principles of healthcare: ethics, compassion, and trust. The importance of protecting patient privacy is increasing as technology continues to change the face of healthcare services. This pledge is a moral obligation that is consistent with the core values of the healthcare industry, not just a compliance tactic.

As a cornerstone, confidentiality creates a safe haven where patients can confide in healthcare professionals with their most intimate health information. In turn, this trust serves as the cornerstone of efficient medical care by permitting candid dialogue, well-informed choices, and a team-based treatment plan. As healthcare digitizes, maintaining the strong privacy of medical records becomes essential to enabling the smooth adoption of cutting-edge technologies and adhering to patient-centered care principles.

The project's commitment to maintaining confidentiality goes beyond the legal and regulatory framework and helps create a healthcare environment that puts the needs of each individual first. When given the assurance that their private information is treated with the highest care and shielded from unwanted access, patients are more likely to participate actively in their healthcare journey. The ethical obligation to protect medical records reflects a dedication to upholding the values of beneficence and non-maleficence as well as patient autonomy and dignity.

The ethical basis of healthcare services is essentially demonstrated by the secrecy of medical records, which serves as more than merely a precaution. It highlights the realization that every medical record is a personal tale, one that embodies vulnerability, trust, and well-being. In the pursuit of better healthcare outcomes, the effective application of confidentiality measures fortifies the changing healthcare environment by bolstering the idea that technology innovations can live in harmony with the timeless values of patient privacy and trust.

**REFERENCES**

[1] Smith, J. "HIPAA and GDPR Compliance in Healthcare Software." Journal of Health Informatics, 15(2), 45-60. (2020)

[2] Brown, A., & Davis, C. "Enhancing Patient Data Security in EHRs." Health Informatics Journal, 12(3), 87-104. (2019).

[3] Johnson, M., & White, S. "Mitigating Insider Threats in Healthcare Institutions." Journal of Health Information Security, 10(1), 30-45. Patel, R., & Lee, H. (2021). "Blockchain for Secure Medical Records: A Case Study." Healthcare Technology Journal, 18(4), 145-162. (2018).

[4] Clark, E., & Turner, L. "Balancing Security and Usability in Healthcare Software." Journal of Health Informatics, 9(4), 120-138. (2017).

[5] Miller, D., & Johnson, K. "Ethical Issues in Patient Data Privacy." Journal of Medical Ethics, 25(3), 75-90. (2019).

[6] Turner, S., & Harris, R. "Data Breaches in Healthcare: Impacts and Responses." Journal of Health Data Management, 14(2), 65-82. (2020).

[7] Siegler M. Sounding Boards. Confidentiality in medicine--a decrepit concept. N Engl J Med. (1982);

[8] Markus AC. Medical confidentiality and records in general practice. Br J Gen Pract. (1991);

[9] Baldry M, Cheal C, Fisher B, Gillett M, Huet V. Giving patients their own records in general practice: experience of patients and staff. Br Med J (Clin Res Ed) (1986);

[10]Weiss BD. Confidentiality expectations of patients, physicians, and medical students. *JAMA.*(1982);

[11]Britten N, Bartholomew J, Morris R, Zander L. Consultants' and patients' views about patient access to their general practice records. *J R Soc Med.*(1991);

[12]Baldry M, Cheal C, Fisher B, Gillett M, Huet V. Giving patients their own records in general practice: experience of patients and staff. *Br Med J (Clin Res Ed)*(1986);

[13]Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. *J Am Med Inform Assoc* (2013);

[14] Siponen M, Mahmood M & Pahnila S, ‘Compliance with Information Security Policies: An Empirical Investigation’, IEEE Computer Society Publish, (2010).

[15] Smith, E & Eloff, JHP, ‘Security in health-care information systems —current trends’, International Journal of Medical Informatics, vol. 54, (1998).

[16] Siponen M, Mahmood M & Pahnila S, ‘Are employees putting your company at Risk by not following information security policies?’, Communications of the ACM, vol. 52, no. 12, pp. 145-147. (2009).

**APPENDIX-A**

**PSUEDOCODE**

**Code for controller:**

// Login User => /api/v1/login

exports.loginUser = catchAsyncErrors(async (req, res, next) => {

const { email, password } = req.body;

//Check if email and password entered by user

if (!email || !password) {

return next(new ErrorHandler("Please enter email and password", 400));

}

//Finding user in Database

const user = await User.findOne({ email }).select("+password");

if (!user) {

return next(new ErrorHandler("Invalid Email and Password", 401));

}

//Check if entered password is correct or not

const isPasswordMatched = await user.comparePassword(password);

if (!isPasswordMatched) {

return next(new ErrorHandler("Entered Password is wrong!", 401));

}

sendToken(user, 200, res);

});

// Forgot Password => /api/v1/password/forgot

exports.forgotPassword = catchAsyncErrors(async (req, res, next) => {

const user = await User.findOne({ email: req.body.email });

if (!user) {

return next(new ErrorHandler("User not found with this email", 404));

}

//Get Reset Token

const resetToken = user.getResetPasswordToken();

await user.save({ validateBeforeSave: false });

//Create Reset Password URL

const resetUrl = `${req.protocol}://${req.get(

"host"

)}/api/v1/password/reset/${resetToken}`;

const message = `Dear ${user.name},\n\nYou recently requested for a password reset from your Vigorous Fitness account.You can find your link below and reset your password easily.\n\n${resetUrl}\n\nIf it wasn't you who requested for a password reset, or accidentally made a request, ignore this email.Worry not, your password won't be changed unless initiated by you.\n\nStay fit!\nTeam Vigorous Health and Fitness.`;

try {

await sendEmail({

email: user.email,

subject: "Account Reset Password",

message,

});

res.status(200).json({

success: true,

message: `Email sent to ${user.email}`,});}

required: [true, 'Please Enter Phone Number'],

maxlength: [10, "Mobile Number cannot exceed 10 digit"],

},

role: {

type: String,

default: 'user',

},

password: {

type: String,

required: [true, 'Please Enter Password'],

minlength: [6, 'Password must be longer than 6 Character'],

select: false //For hiding the text in input field

},

createdAt: {

type: Date,

default: Date.now

},

resetPasswordToken: String,

resetPasswordExpire: Date

})

module.exports = mongoose.model('User', userSchema)

//Encrypting Password before saving the user

userSchema.pre('save', async function (next) {

//Checking if password is modified or not

if (!this.isModified('password')) {

next()

}

this.password = await bcrypt.hash(this.password, 10)

})

**Code for Models:**

const patientSchema = new mongoose.Schema({

name: {

type: String,

required: [true, 'Please Enter Patient Name'],

maxlength: [30, 'Patient name cannot exceed more than 30 Characters']

},

dob: {

type: Date,

required: [true, 'Please Enter Date of Birth']

},

sex: {

type: String,

enum: ['Male', 'Female', 'Other'],

required: [true, 'Please Enter Patient Sex']

},

bloodGroup: {

type: String,

required: [true, 'Please Enter Blood Group']

},

phoneNumber: {

type: Number,

required: [true, 'Please Enter Phone Number'],

maxlength: [10, 'Mobile Number cannot exceed 10 digits']

},

alternateNumber: {

type: Number,

maxlength: [10, 'Alternate Number cannot exceed 10 digits']

},

insuranceCarrier: {

type: String,

required: [true, 'Please Enter Insurance Carrier']

},

policyNumber: {

type: String,

required: [true, 'Please Enter Policy Number']

},

pastConditions: {

type: String

},

surgeries: {

type: String

},

medications: [{

name: {

type: String,

required: [true, 'Please Enter Medication Name']

},

dosage: {

type: String,

required: [true, 'Please Enter Dosage']

},

frequency: {

type: String,

required: [true, 'Please Enter Medication Frequency']

},

physician: {

type: String,

required: [true, 'Please Enter Physician Name']

}

}],

createdAt: {

type: Date,

default: Date.now

}

});

**Code for Routing:**

const express = require('express')

const router = express.Router();

const {isAuthenticatedUser, authorizeRoles} = require('../middleware/auth')

const {

registerUser, loginUser, logout,

forgotPassword, resetPassword, currentUser,

updatePassword, updateProfile, allUsers,

getUserDetails, updateUser, deleteUser

} = require('../controllers/authControllers')

router.route('/login').post(loginUser)

router.route('/logout').get(logout)

router.route('/password/forgot').post(forgotPassword)

router.route('/password/reset/:token').put(resetPassword)

router.route('/currentUser').get(isAuthenticatedUser, currentUser)

router.route('/profile/update\_password').put(isAuthenticatedUser, updatePassword)

router.route('/profile/edit\_profile').put(isAuthenticatedUser, updateProfile)

router.route('/admin/register').post(isAuthenticatedUser, authorizeRoles('admin'),registerUser)

router.route('/admin/all\_users').get(isAuthenticatedUser, authorizeRoles('admin'), allUsers)

router.route('/admin/users/:id')

.get(isAuthenticatedUser, authorizeRoles('admin'), getUserDetails)

.put(isAuthenticatedUser, authorizeRoles('admin'), updateUser)

.delete(isAuthenticatedUser, authorizeRoles('admin'), deleteUser)

module.exports = router;

const express = require('express');

const router = express.Router();

const { isAuthenticatedUser, authorizeRoles } = require('../middleware/auth');

const {

addPatient,

getAllPatients,

getPatientById,

updatePatient,

deletePatient

} = require('../controllers/patientControllers');

// Middleware to protect routes

router.use(isAuthenticatedUser);

// Routes for patient operations

router.route('/patients')

.post(authorizeRoles('admin'), addPatient) // Add a new patient

.get(authorizeRoles('admin'), getAllPatients); // Get all patients

router.route('/patients/:id')

.get(authorizeRoles('admin'), getPatientById) // Get a specific patient by ID

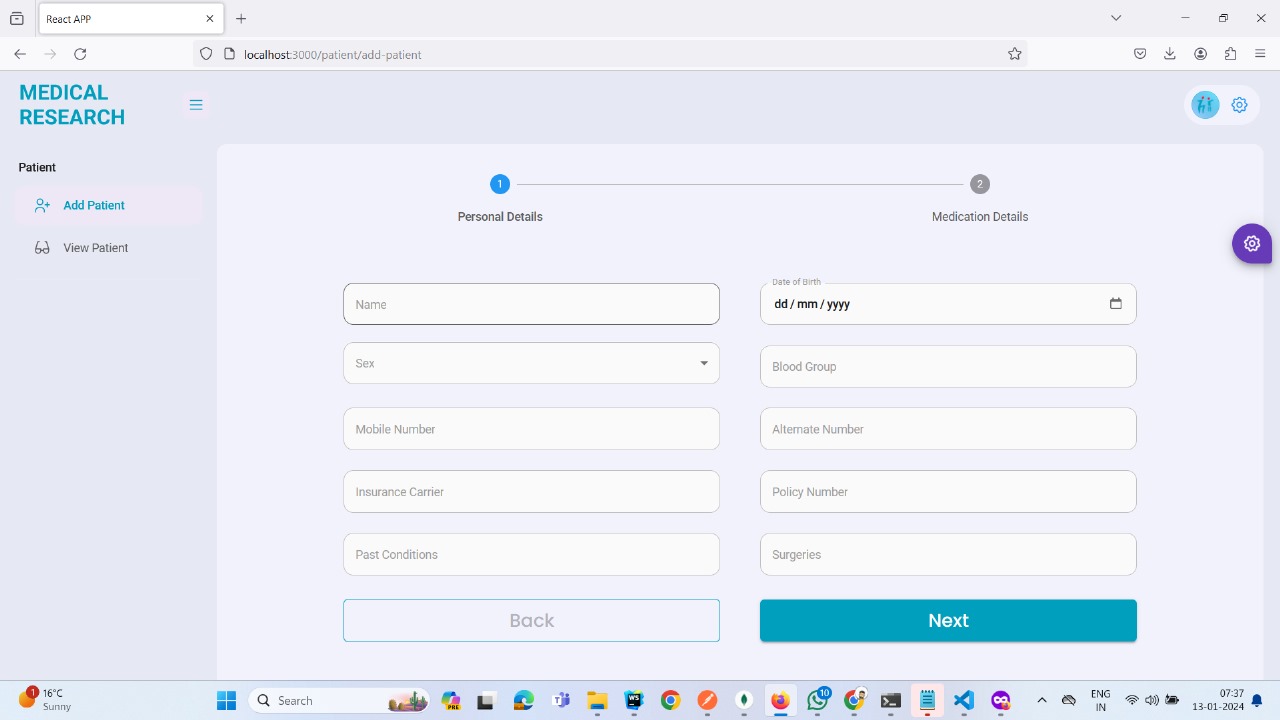
.put(authorizeRoles('admin'), updatePatient) // Update a patient

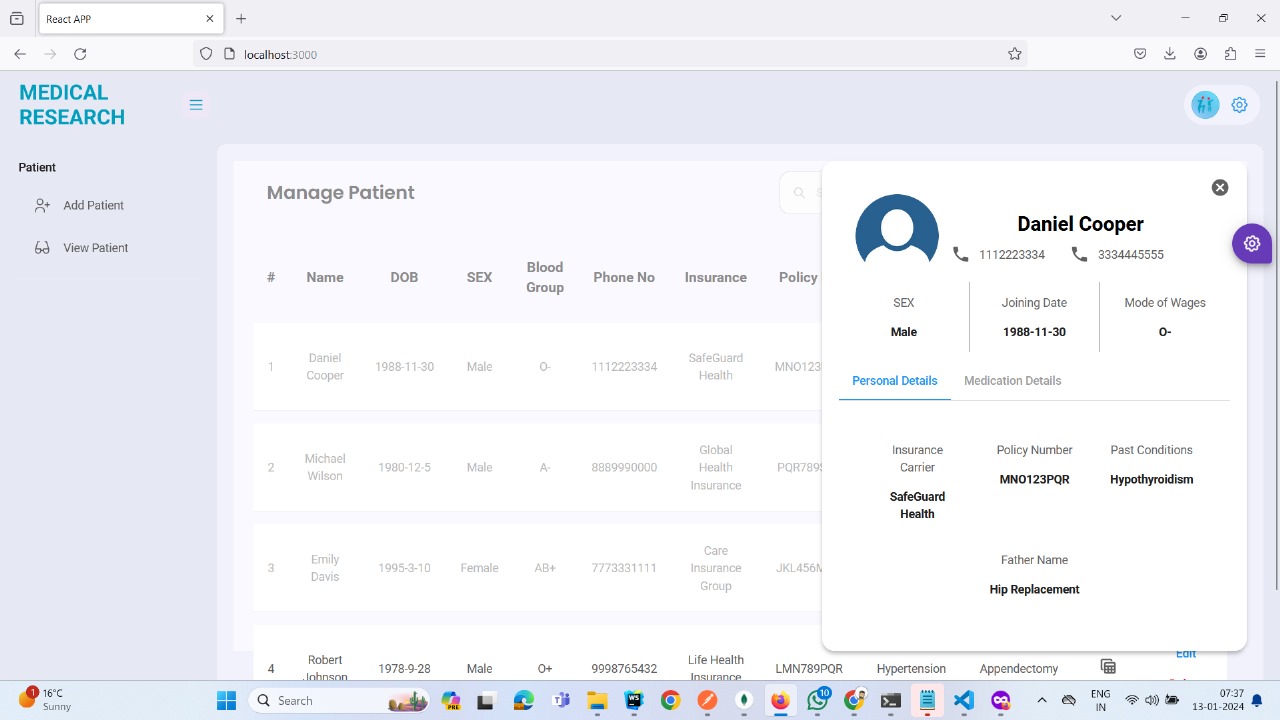
.delete(authorizeRoles('admin'), deletePatient); // Delete a patient

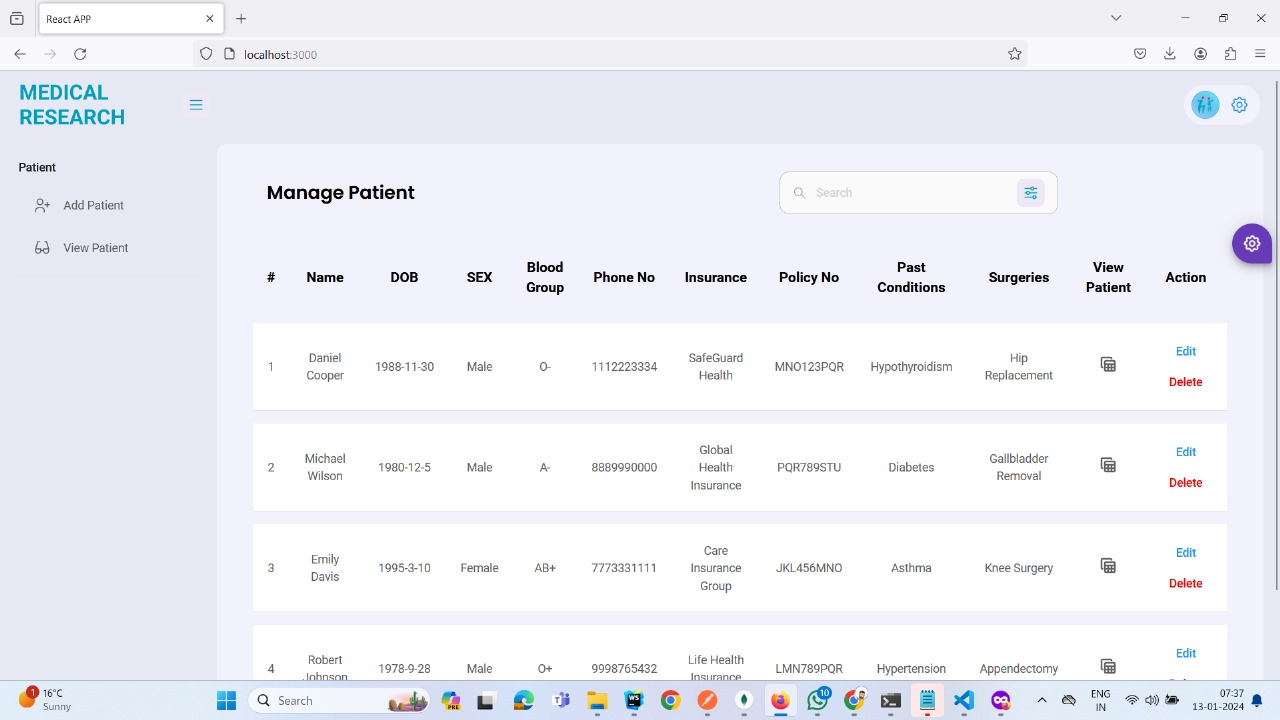
module.exports = router;

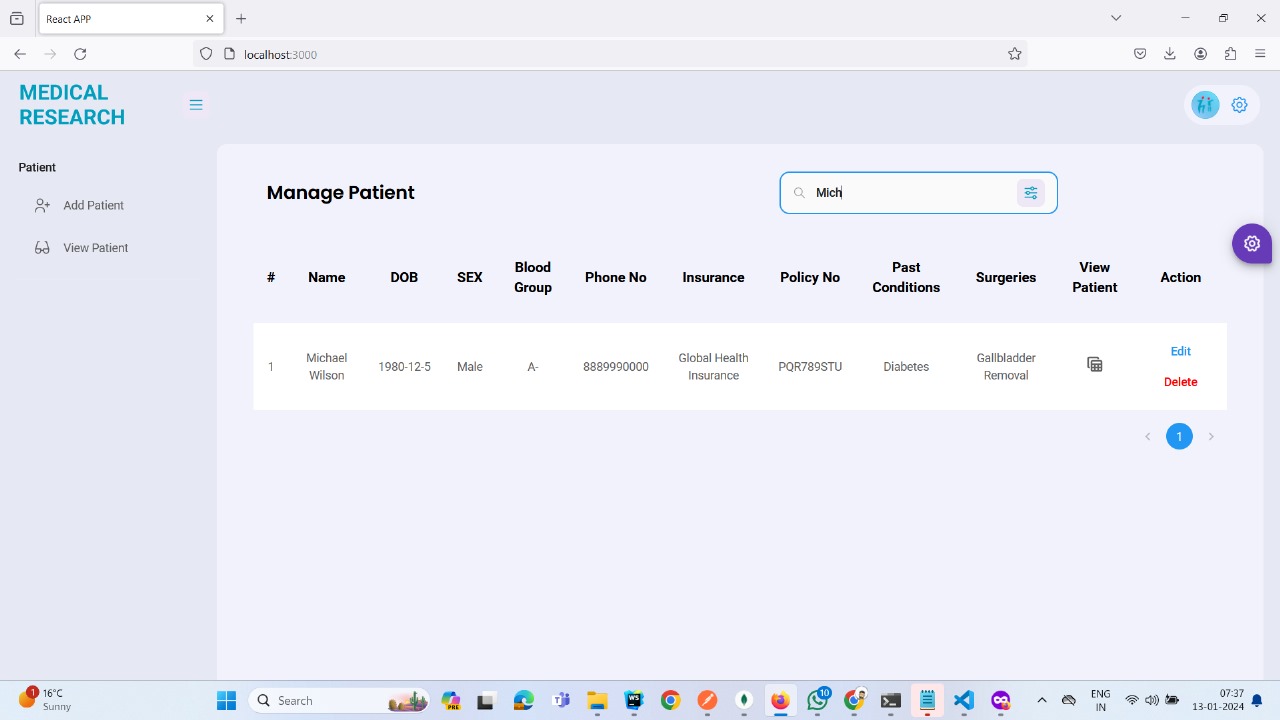
**APPENDIX-B**

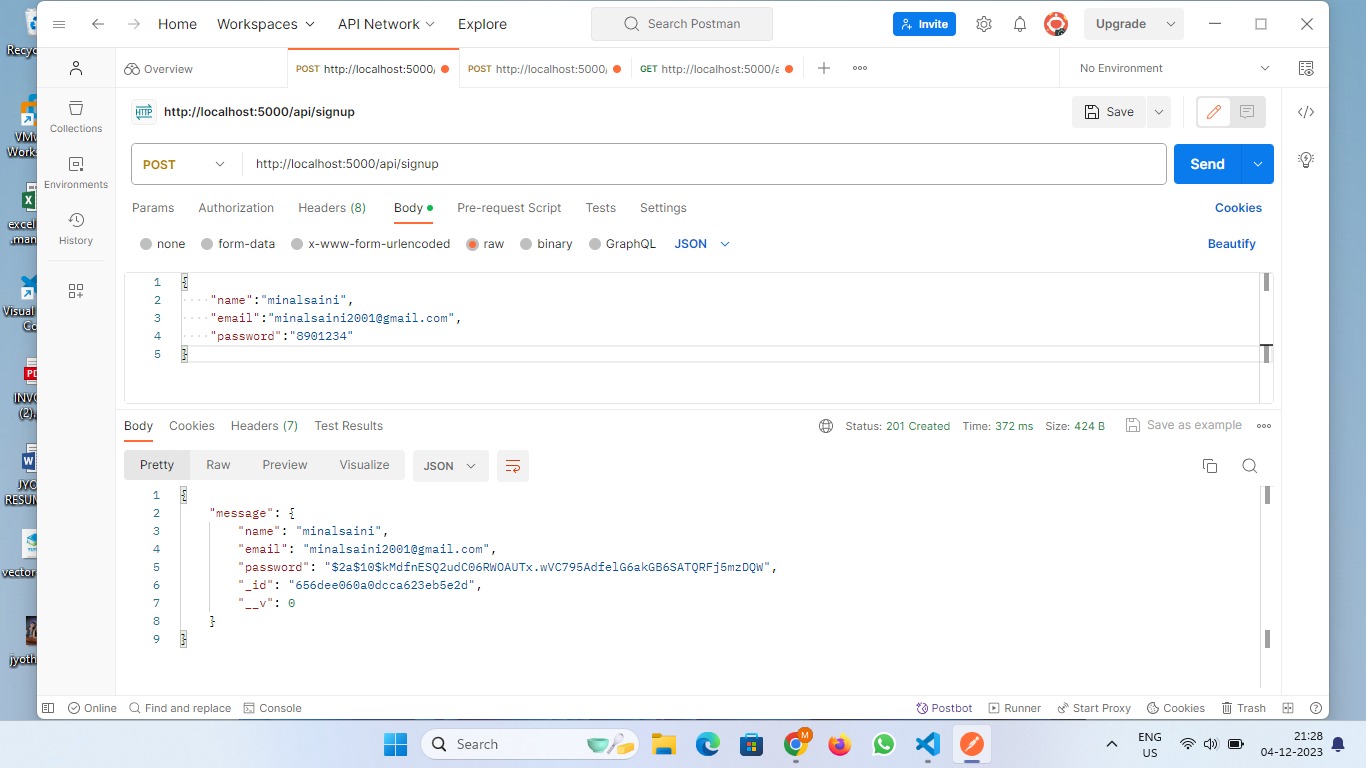
**SCREENSHOTS**

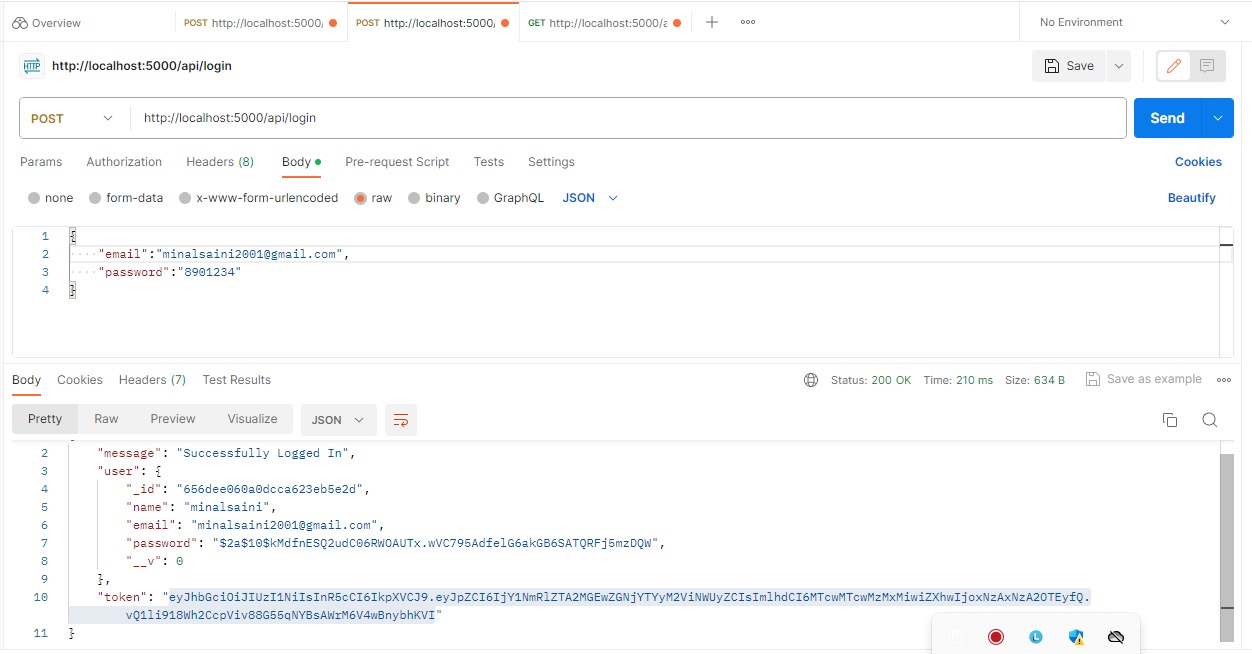


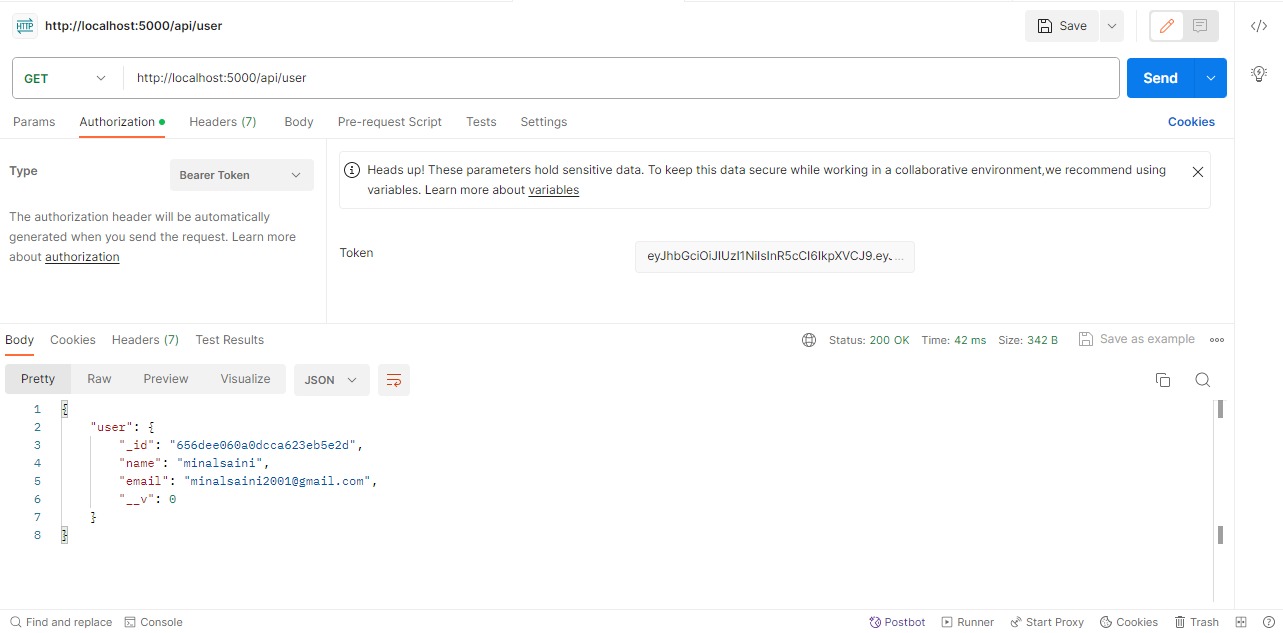




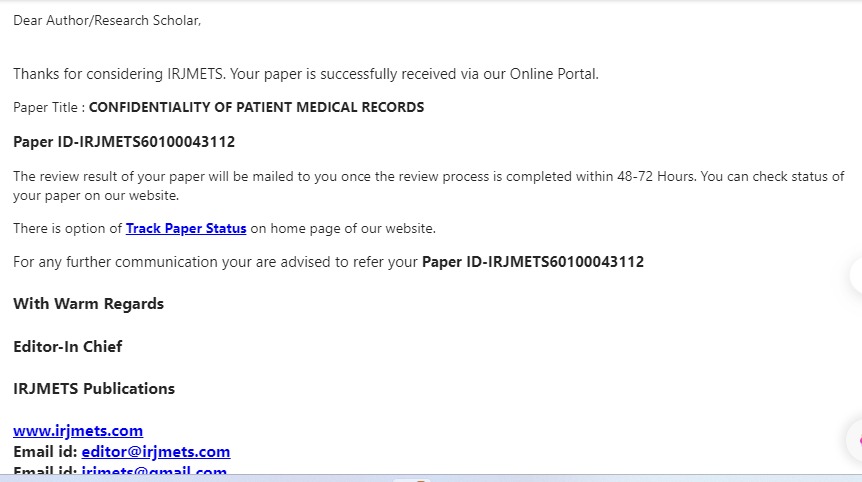




****



**APPENDIX-C**

****

****

**SDG - SUSTAINABLE DEVELOPMENT GOALS**

****

**The project work carried out here is named to SDG - 3 good health and well-being.**

By enhancing patient privacy and confidence, Our project that prioritizes patient medical record confidentiality directly contributes to the achievement of SDG Goal 3. This program encourages early intervention and illness prevention by ensuring people feel comfortable sharing sensitive health information. The project's efforts to protect patient data are in line with SDG Goal 3's aims, which include promoting a healthcare environment that prioritizes individual well-being, lowering stigma, and guaranteeing healthy lives.

