Department of Electrical and Computer Engineering

North South University

Senior Design Project

MedEase

Blockchain based Electronic Healthcare System

Chowdhury Nafis Faiyaz, ID- 1931841642

Ayman Ibne Hakim, ID- 2103364042

Faculty Advisor:

Mohammad Ashrafuzzaman Khan

Assistant Professor

ECE Department

Summer, 2023

LETTER OF TRANSMITTAL

June, 2023

To

Dr. Rajesh Palit

Chairman,

Department of Electrical and Computer Engineering

North South University, Dhaka

Subject: **Submission of Capstone Project Report on "MedEase Blockchain based Electronic Healthcare System"**

Dear Sir,

With due respect, we would like to submit our **Capstone Project Report** on **"MedEase-Blockchain based Electronic Healthcare System"** as a part of our BSc program. The report deals with a blockchain based electronic medical health care system. This project was very much valuable to us as it helped us gain experience from practical fields and apply in real life. We tried to the maximum competence to meet all the dimensions required from this report.

We will be highly obliged if you kindly receive this report and provide your valuable judgment. It would be our immense pleasure if you find this report useful and informative to have an apparent perspective on the issue.

Sincerely Yours,

....
Chowdhury Nafis Faiyaz
ECE Department
North South University, Bangladesh

....
Ayman Ibne Hakim
ECE Department
North South University, Bangladesh

APPROVAL

Chowdhury Nafis Faiyaz (ID # 1931841642) And Ayman Ibne Hakim (ID # 2103364042) from Electrical and Computer Engineering Department of North South University, have worked on the Senior Design Project titled "**MedEase- Blockchain based Electronic Healthcare System**" under the supervision of Mohammad Ashrafuzzaman Khan partial fulfillment of the requirement for the degree of Bachelors of Science in Engineering and has been accepted as satisfactory.

Supervisor's Signature

…………………………………….

Mohammad Ashrafuzzaman Khan

Assistant Professor

Department of Electrical and Computer Engineering

North South University

Dhaka, Bangladesh.

Chairman's Signature

…………………………………….

Dr. Rajesh Palit

Professor

Department of Electrical and Computer Engineering

North South University

Dhaka, Bangladesh.

DECLARATION

This is to declare that this project is our original work. No part of this work has been submitted elsewhere partially or fully for the award of any other degree or diploma. All project related information will remain confidential and shall not be disclosed without the formal consent of the project supervisor. Relevant previous works presented in this report have been properly acknowledged and cited. The plagiarism policy, as stated by the supervisor, has been maintained.

Students' names & Signatures

....	....
Chowdhury Nafis Faiyaz	Ayman Ibne Hakim
ECE Department	ECE Department
North South University, Bangladesh	North South University, Bangladesh

ACKNOWLEDGEMENTS

The authors would like to express their heartfelt gratitude towards their project and research supervisor, Mohammad Ashrafuzzaman Khan, Assistant Professor, Department of Electrical and Computer Engineering, North South University, Bangladesh, for his invaluable support, precise guidance and advice pertaining to the experiments, research and theoretical studies carried out during the course of the current project and also in the preparation of the current report.

Furthermore, the authors would like to thank the Department of Electrical and Computer Engineering, North South University, Bangladesh for facilitating the research. The authors would also like to thank their loved ones for their countless sacrifices and continual support.

ABSTRACT

MedEase

Blockchain based Electronic Healthcare System

The healthcare industry is witnessing a digital transformation with the advent of blockchain technology, offering an innovative approach to managing electronic health records (EHRs) and healthcare data. This abstract presents an overview of the potential benefits, challenges, and implications of implementing a blockchain-based electronic healthcare system.

Blockchain technology's core features, including decentralization, immutability, transparency, and cryptographic security, make it an ideal solution for healthcare data management. This system offers a tamper-proof and secure environment for storing, sharing, and accessing patient information. Healthcare providers, patients, and other authorized stakeholders can access EHRs with reduced concerns about data breaches, unauthorized access, or fraudulent activities.

Moreover, the use of smart contracts within blockchain-based healthcare systems automates various administrative processes, such as consent management, and data sharing agreements. This automation streamlines operations, reduces human error, and enhances overall efficiency in healthcare. However, blockchain-based healthcare systems face certain challenges, including scalability, interoperability, and regulatory compliance. Scalability is crucial as the system must handle a vast amount of healthcare data efficiently. Interoperability is essential to ensure that various healthcare institutions and systems can communicate and share data securely.

In conclusion, a blockchain-based electronic healthcare system has the potential to revolutionize the healthcare industry by improving data security, streamlining operations, and increasing transparency. While challenges remain, addressing scalability, interoperability, and regulatory compliance will be essential to realizing the full potential of blockchain technology in

healthcare. The adoption of such systems promises a future where patients and healthcare providers can trust that sensitive medical data is secure, accessible, and efficiently managed, ultimately leading to improved patient care and outcomes.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1 Introduction

1.1 Background and Motivation

1.2 Background-

Electronic Health Records (EHRs) have emerged as a pivotal advancement in the healthcare industry, replacing traditional paper-based medical records with digital counterparts. This transformation stems from the need to overcome several longstanding challenges in healthcare management. The paper-based record-keeping systems were notorious for being error-prone, inefficient, and often plagued by issues of accessibility and security. They also failed to facilitate the exchange of medical information between different healthcare providers and stakeholders, hindering continuity of care and patient safety. Our aim with this project is to introduce a system where the users (patients, doctors, administrations) can use our platform to seamlessly deliver a service to the patients. We have focused on securely storing confidential patient data by using a tamper proof, decentralized blockchain system.

1.3 Motivation-

The motivation behind Electronic Health Records (EHRs) lies in addressing critical challenges within the healthcare industry. EHR adoption is driven by the need to:

1. Enhance Patient Care: EHRs improve access to vital patient information, enabling more informed clinical decisions and reducing medical errors, ultimately leading to better patient care.
2. Streamline Care Coordination: EHRs facilitate seamless communication among healthcare providers, ensuring consistent and coordinated care for patients, especially in complex medical cases.
3. Ensure Data Security: EHRs offer robust security measures, safeguarding patient data and reducing vulnerabilities to breaches, a pressing concern in healthcare.
4. Boost Efficiency: Automation of administrative tasks, such as billing and appointment scheduling, increases operational efficiency, reducing errors and cutting costs.

5. Contribute to Research: EHRs enable data sharing for medical research and public health efforts, fostering medical advancements and informed healthcare policies.
6. Regulatory Compliance: Compliance with healthcare regulations and standards is a driving force, as non-compliance can result in penalties and loss of accreditation.
7. Engage Patients: EHRs empower patients to take a more active role in their healthcare, fostering patient-centered approaches and shared decision-making.

In summary, EHR adoption aims to revolutionize healthcare by improving care quality, security, efficiency, research contributions, and patient engagement. It represents a fundamental shift towards a more effective and patient-centric healthcare ecosystem

1.4 Purpose and Goal of the Project

The objective of this project is to develop a web application using IPFS and private blockchain to provide a secure and efficient way for patients to manage their medical records. Additionally, we also aim to provide features like booking online and offline appointments, booking hospital beds, and ordering medicine from pharmacies.

1.5 Organization of the Report

Here's a brief overview of the purpose and content of each chapter in the document you provided:

Chapter 1: Introduction

- Background and Motivation (Section 1.1): Sets the context for the project and explains the reasons behind undertaking it.
- Purpose and Goal of the Project (Section 1.4): Clearly defines the objectives and desired outcomes of the project.
- Organization of the Report (Section 1.5): Outlines the structure of the entire document, giving readers an overview of what to expect.

Chapter 2: Research Literature Review

- Existing Research and Limitations (Section 2.1): Reviews prior research in the field, highlighting both what has been achieved and the gaps or limitations in the existing knowledge.

Chapter 3: Methodology

- System Design (Section 3.1): Describes the design of the system, including elements like Class and UseCase diagrams.
- Hardware and/or Software Components (Section 3.2): Provides information on the technical components that will be used in the project.

Chapter 4: Investigation/Experiment, Result, Analysis, and Discussion

- Presents the results of the research, experiments, or investigations conducted as part of the project.
- Includes visual representations, like Figures 4.1 and 4.2, which may illustrate key processes or findings.

Chapter 5: Impacts of the Project

- Analyzes the broader societal, health, safety, legal, cultural, and environmental impacts that the project may have.

Chapter 6: Project Planning

- Likely includes a Gantt chart (as mentioned in Figure 1) to detail the project timeline and milestones.

Chapter 7: Complex Engineering Problems and Activities

- Discusses the complex engineering problems (CEP) and activities (CEA) encountered during the project, potentially offering insights into the challenges faced and solutions developed.

Chapter 8: Conclusions

- Summarizes the main findings and outcomes of the project.
- Discusses any limitations encountered during the project.
- Provides suggestions for future improvements or research directions.

Each chapter serves a specific purpose in documenting and presenting the research project, offering readers a structured and comprehensive understanding of the project's scope, progress, and potential impacts.

Chapter 2 Research Literature Review

2.1 Existing Research and Limitations

Xia et al. [1] developed a blockchain-based system called MeDShare that addresses the issue of medical data sharing among medical big data custodians in a trust-less environment. MeDShare uses blockchain technology to address these challenges. It uses smart contracts to track the behavior of the data and revoke access to offending entities. By implementing MeDShare, cloud service providers and other data guardians will be able to achieve data provenance and auditing while sharing medical data with entities such as research and medical institutions with minimal risk to data privacy. However, they are storing data in cloud services, which is less secure compared to our proposed solution which is IPFS. Moreover, sharing data among multiple hospitals is not possible in this system compared to ours where data can be shared with any registered hospital after taking the patient's consent.

Azaria et al. [2] developed MedRec- a system that addresses these challenges by using blockchain technology. In a blockchain based system, data is stored in blocks that are linked together in a chain. The MedRec system also gives patients more control over their medical data. They have used a public blockchain, meaning anyone with access to that block can see the hashes of the EHR chunks. Our system will be built using a private blockchain which means no outsider will be able to get access to the block, thus, making it more secure. Additionally, in our system, the files will be stored in IPFS which is a more secure and environment friendly solution.

Bowles et al. [3] discuss a blockchain-based platform for sharing medical data in a secure and personalized way. It describes the proposed blockchain-based platform for sharing medical data. The platform consists of the following components:

- A private blockchain: The private blockchain is used to store the medical data. The blockchain is maintained by a group of authorized participants, such as healthcare organizations and patients.
- Smart contracts: Smart contracts are used to control access to the medical data. Smart contracts are self-executing contracts that are stored on the blockchain. They can be used to define who has access to the medical data and what they can do with it.

- A data encryption scheme: The medical data is encrypted before it is stored on the blockchain. This helps to protect the confidentiality of the information.

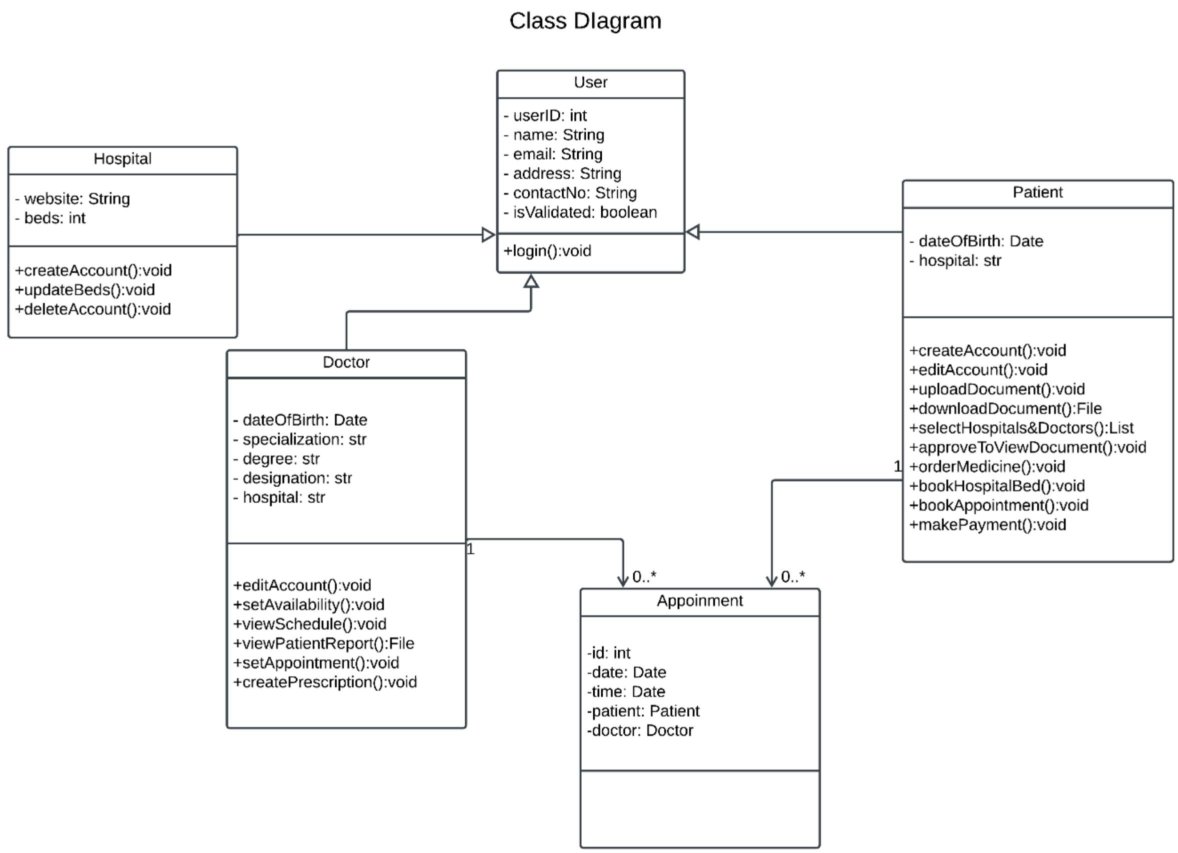
Although this solution works well, storing large amounts of data on blockchain is not recommended since it uses a high amount of energy. In our planned system, we will be using IPFS to store the files, and use private blockchain to store the hash of the file.

Khan et al. [4] developed a similar system as we propose using JavaScript, React, HTML and Solidity. All of the patients' submitted records will be kept on their local server (Ganache). The records are kept in the form of hashed strings containing the data. Additionally, each file will have a unique Uniform Resource Locator (URL) that will be shown in the patient's profile. There will also be an option for patients to give physicians access to their medical records. After being granted access, physicians will be able to see their records in their profile. To get access to features such as uploading, viewing, or modifying data. Similar to MedRec, they have stored the files inside the blockchain which is not environment friendly and also makes the application slow. Our proposed system will use IPFS to store the files making it a more environment friendly solution.

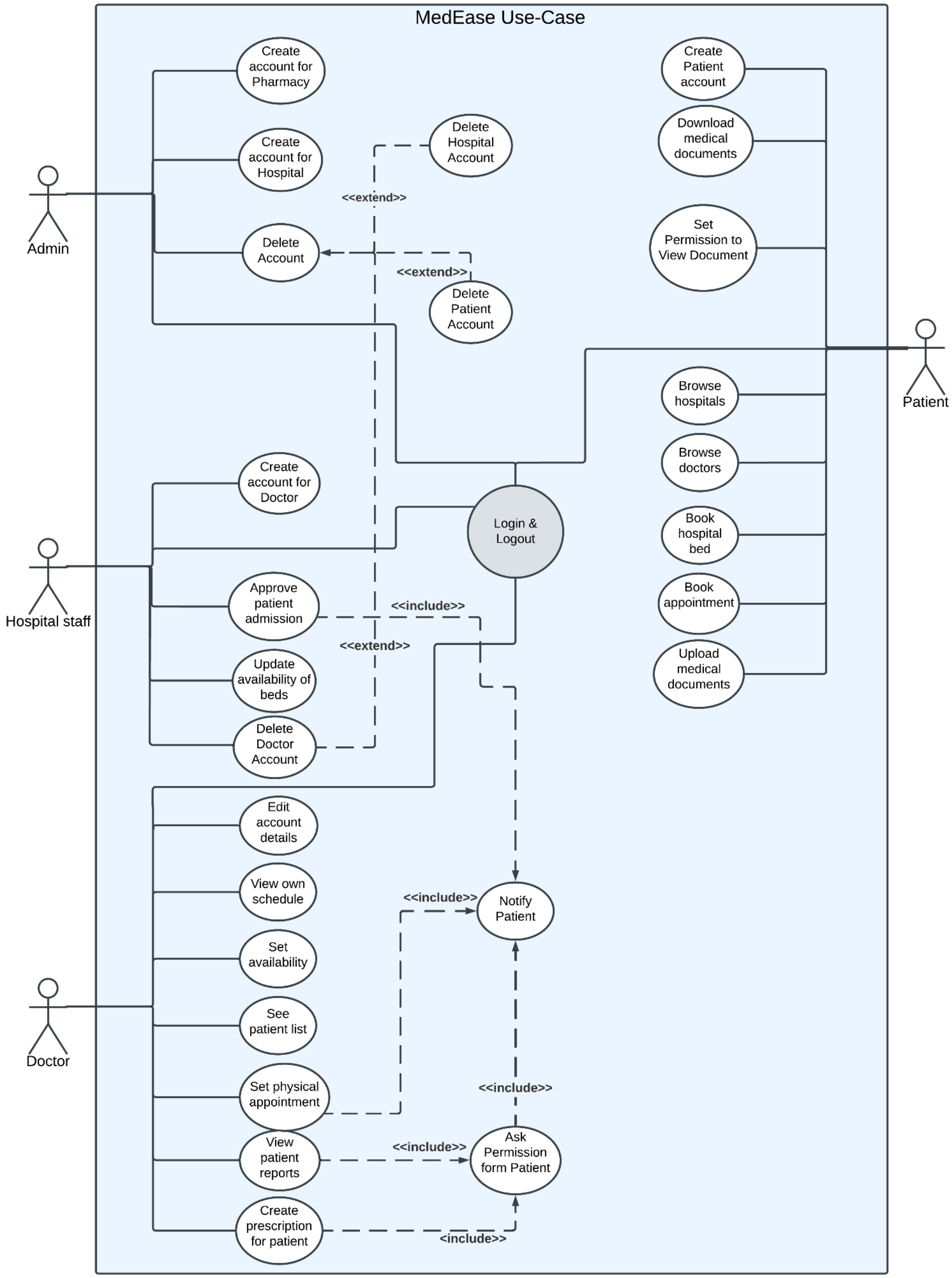
Chapter 3 Methodology

3.1 System Design

3.1.1 Class Diagram



3.1.2 UseCase Diagram



3.2 Hardware and/or Software Components

The software component of this healthcare system, developed with a technology stack comprising React, Next.js, Tailwind CSS, Node.js, IPFS, and blockchain, plays a pivotal role in revolutionizing patient data and medical report management. React and Next.js, together with Tailwind CSS, provide a robust and responsive user interface, offering a seamless and intuitive user experience for healthcare professionals and patients alike. Node.js powers the backend, ensuring efficient data processing and management. However, the most innovative aspect of this system lies in its utilization of blockchain technology for storing patient data and reports.

Blockchain provides a secure, transparent, and tamper-proof environment for sensitive medical information. Patient records and reports are encrypted and stored on the blockchain, ensuring that only authorized users can access them, thereby enhancing data security and privacy. Immutability and cryptographic mechanisms guarantee the integrity of the stored data, making it resistant to unauthorized alterations or breaches. The use of smart contracts streamlines administrative processes, such as consent management and data sharing agreements, further enhancing operational efficiency.

This software component represents a cutting-edge solution in healthcare data management, offering the combined benefits of a user-friendly interface, efficient data processing, and the unparalleled security and transparency of blockchain technology. It ultimately contributes to better patient care, streamlined operations, and a trustworthy and efficient healthcare ecosystem.

Table I. List of Software/Hardware Tools

Tool	Functions	Other similar Tools (if any)	Why selected this tool
React and tailwind css	Front end development	Vue.js	
Node.js	Backend development	Python, Java	Runs faster
IPFS	Storing patient Data		Secure for storing files
Hyperledger Fabric	Storing hash of the files and smart contracts		Popular for implementing private blockchain network

Chapter 4 Investigation

In our application, the EHRs will be stored on IPFS. The hash of the file returned by the IPFS will be stored on a private blockchain.

The InterPlanetary File System (IPFS) is a distributed file system that allows users to store and share files in a peer-to-peer manner. IPFS is designed to be a more efficient and reliable alternative to traditional file sharing systems, such as HTTP and BitTorrent. IPFS works by storing files in a decentralized manner, meaning that files are not stored on a single server, but rather on a network of computers. When a user wants to download a file, IPFS will connect to the nearest nodes that have that file and download it from them. IPFS uses Content Addressing (CA), a unique addressing technique. The content of the file, not its location, determines the CA address. This implies that a file's CA address remains unchanged even if it is transferred to a new place. CA addresses are calculated using a cryptographic hash function. This means that the CA address of a file is unique and cannot be tampered with. IPFS uses a data structure, Merkle DAG, for efficient and scalable file storage. It is a tree-like structure with each node representing a data chunk, and the root node representing the entire file, allowing for file integrity verification. Once a file has been uploaded, the IPFS will return the hash of the file to the client which will be stored in a private blockchain

Blockchain technology stores information in blocks that are connected to create an eternal record. Every block has a list of transactions, a timestamp, and a cryptographic hash of the block before it. Data manipulation is highly difficult since each block is uniquely connected to the preceding block because of the cryptographic hash. Once a transaction is added to a block, it is verified by the nodes on the network. If the transaction is valid, it is added to the blockchain and cannot be changed or deleted. This makes blockchain ideal for storing medical records. A smart contract will be deployed to the network which will manage the storage and access of the files. A smart contract is a self-executing contract that is stored on a blockchain. Smart contracts can be used to automate transactions and create complex agreements. In our software smart contracts will be used to manage the hash storage and access of the files.

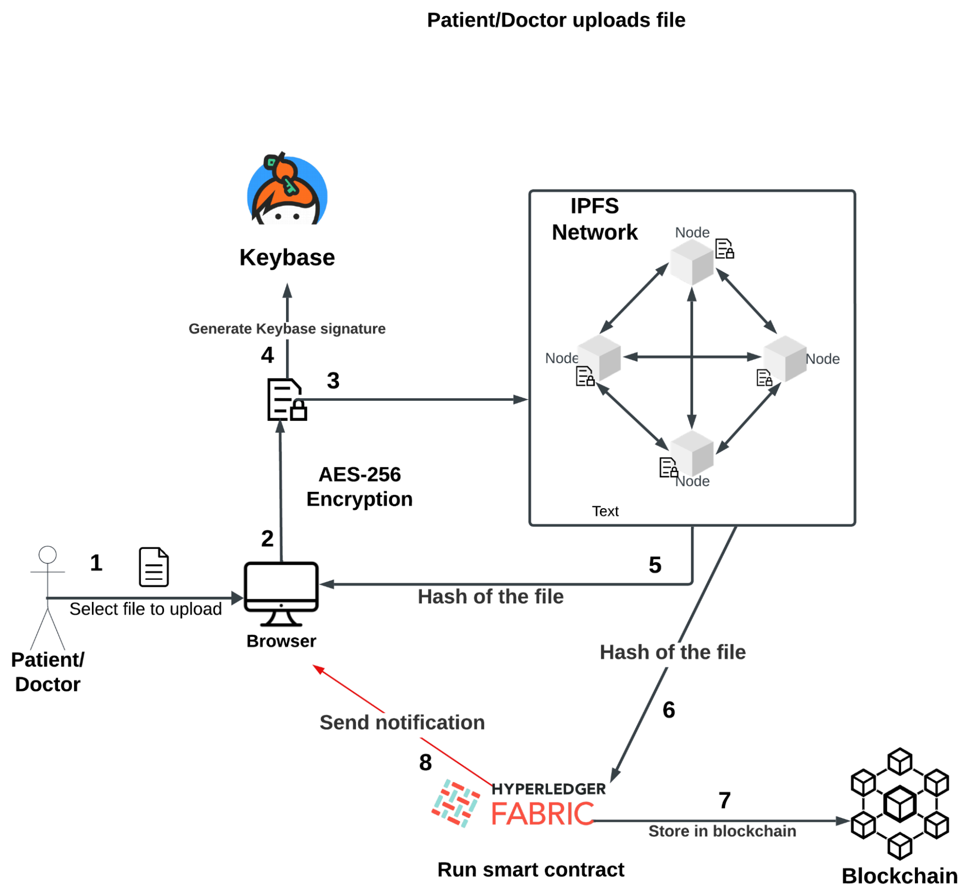


Figure 4.1 : Storing files

Figure 4.1 shows the flow of how the file storage mechanism works. When the patient/doctor selects a file and clicks upload, the browser takes the file and generates a random 256-bit AES encryption key and uses it to encrypt the file. The browser then generates a Keybase signature for the encrypted file and stores the signature in the file's metadata. The encrypted file is then sent to the IPFS where the file is broken down into smaller chunks and each chunk is stored on a different node. The IPFS generates a hash of the file using SHA-256 cryptographic algorithm and sends the hash to the smart contract which is run on Hyperledger Fabric on a private blockchain. Upon receiving the hash of the file, the smart contract creates a new transaction that contains the hash of the file. The transaction is then submitted to the blockchain network. The blockchain network then validates the transaction and adds it to the blockchain. The smart contract then returns the transaction ID to the client application. Similarly, another smart contract will run that stores the files metadata. The smart contract will create a new transaction that contains the file's metadata. The smart contract which contains the list of all the patient's files' metadata validates the transaction and adds the new file's metadata to the list and finally returns the transaction ID to the client.

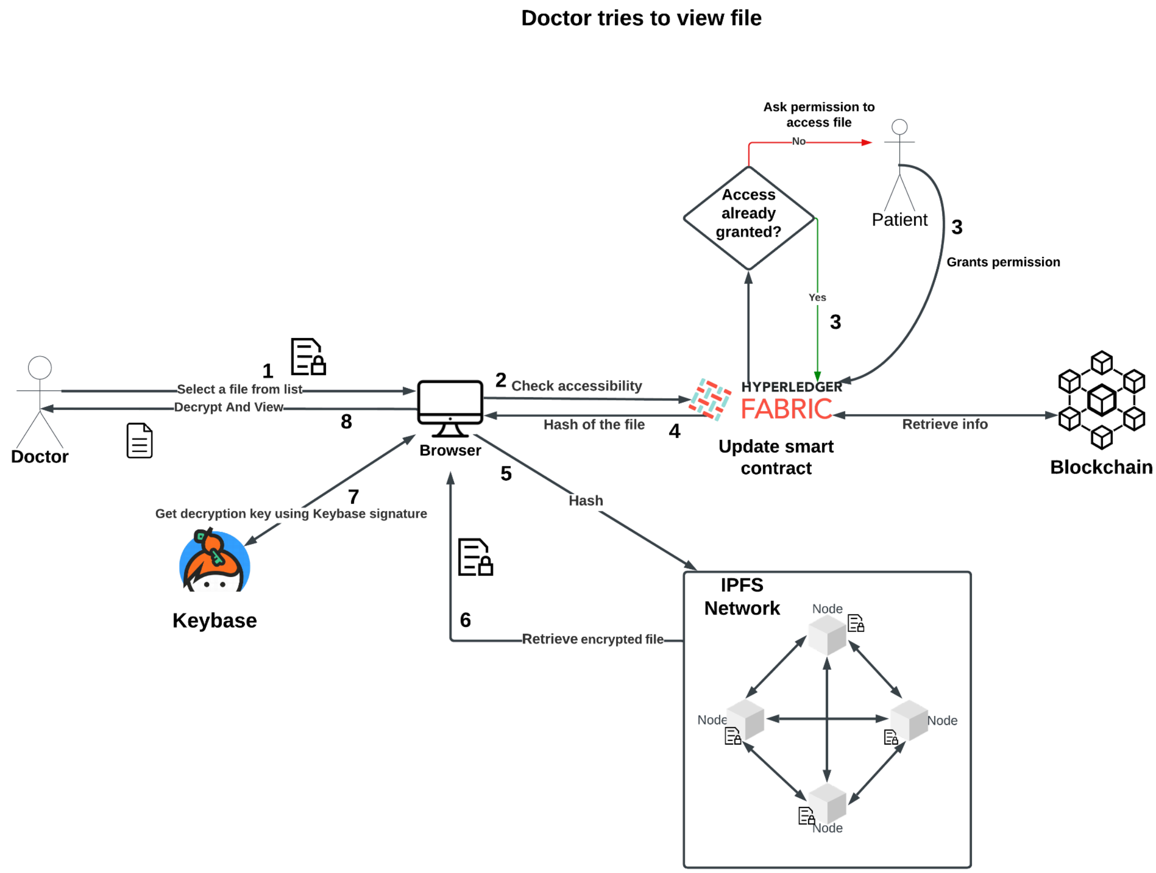


Figure 4.2 : Doctor retrieving a patient record

Figure 4.2 shows the flow of the software when a doctor tries to view a patient's record. When the doctor clicks on a 'View Document' button, the browser sends a request to the smart contract to request permission to view the file. The request includes the hash of the file and the doctor's address. To confirm that the doctor has permission to view the file, the smart contract validates the request. The smart contract also verifies that the file exists in IPFS. If the request is valid, the smart contract sends a notification to the owner of the file. If the request is rejected, a message will be shown on the screen stating access denied. If the owner grants permission, the owner signs a transaction that grants the doctor access to the file. The smart contract updates the access control list for the file to grant permission to the doctor. Using the hash, the encrypted file is retrieved from the IPFS. Using the Keybase signature, the decryption key is retrieved and used to decrypt the file. Finally, the decrypted file is viewed on the screen.

Chapter 5 Impacts of the Project

5.1 Impact of this project on societal, health, safety, legal and cultural issues

The adoption of electronic medical records (EHRs) has multifaceted social effects. Firstly, EHRs significantly enhance patient care by facilitating quick and accurate access to medical information, resulting in faster diagnoses, reduced errors, and improved treatment outcomes, thereby elevating overall healthcare quality. Moreover, they streamline administrative tasks, such as appointment scheduling and billing, increasing operational efficiency, reducing wait times, and allowing healthcare professionals to prioritize patient care. However, the digital nature of EHRs raises valid concerns about data security and patient privacy, necessitating robust cybersecurity measures and regulatory compliance to safeguard sensitive information. Nevertheless, the widespread adoption of EHRs may inadvertently exacerbate health care access disparities, as individuals lacking internet access or digital literacy skills encounter barriers to using these systems. This calls for healthcare organizations to provide alternative solutions for underserved populations. Additionally, healthcare professionals must adapt to EHRs, potentially requiring training and adjustment to new workflows, with the transition impacting job satisfaction and work-life balance for some. Lastly, ethical considerations arise regarding data ownership, consent, and the potential misuse of patient information. Healthcare providers must adhere to ethical guidelines and transparent data practices to maintain trust with patients.

5.2 Impact of this project on environment and sustainability

The adoption and utilization of electronic medical record (EHR) healthcare web applications have discernible environmental effects. Chief among these is the significant reduction in paper usage, mitigating the environmental impact associated with the extensive use of paper in traditional medical records, which leads to deforestation and heightened energy consumption for printing and storage. Furthermore, EHRs necessitate data centers and servers for the storage and management of patient data, which consume energy for their operation and cooling. Nonetheless, when compared to the energy-intensive maintenance of paper records, EHRs tend to have a lower overall environmental impact, particularly when data centers employ renewable energy sources. Nevertheless, the continual upgrading and replacement of hardware and software components in EHRs contribute to electronic waste (e-waste), underlining the importance of proper disposal and recycling of outdated equipment like hardware, batteries, and electronic chips to mitigate this environmental concern. Additionally, the carbon emissions from data centers hosting healthcare web applications are contingent on factors such as their energy efficiency and the source of their electricity.

Chapter 6 Project Planning

Proposed execution timeline for MedEase

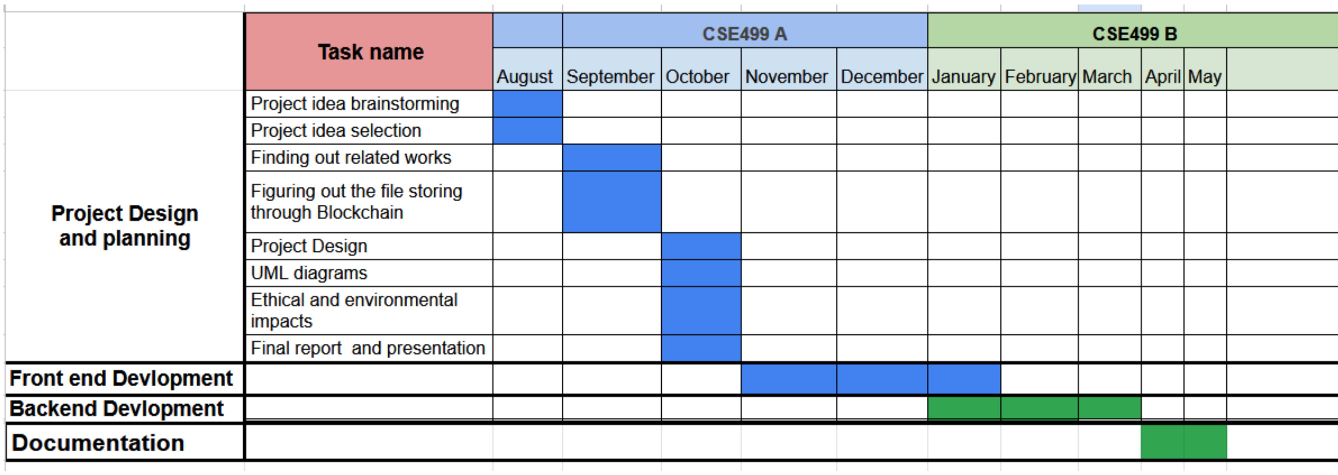


Figure 1. A sample Gantt chart.

Chapter 7 Complex Engineering Problems and Activities

7.1 Complex Engineering Problems (CEP)

Table I. A Sample Complex Engineering Problem Attributes

Attributes		**Addressing the complex engineering problems (P) in the project**
P1	Depth of knowledge required	The project requires knowledge of web application development, IPFS technology, blockchain technology, system security, and database management.
P2	Range of conflicting requirements	The application must be secure to protect patient privacy, but it must also be performant so that healthcare professionals can access patient records quickly and easily.
P3	Depth of analysis required	• The healthcare industry • The different roles and permissions of healthcare professionals • The different types of patient data that need to be managed • The security and privacy requirements for patient data
P4	Familiarity of issues	The challenges of integrating blockchain technology and IPFS into a web application
P5	Extent of stakeholder involvement	There are several stakeholders needs to be involved including patients, doctors, and Healthcare organizations

7.2 Complex Engineering Activities (CEA)

Table III. A Sample Complex Engineering Problem Activities

Attributes		**Addressing the complex engineering activities (A) in the project**
A1	Range of resources	This project involves human resource, money, modern tools (simulation software/mobile APP).
A2	Level of interactions	Involves interactions between different stakeholders including patients, doctors, healthcare organizations, and pharmacies.
A3	Innovation	Employs innovative skills of engineering by introducing technology in a different manner in the healthcare sector
A4	Consequences to society / Environment	Makes it easier to manage and share medical records with doctors. Impact in our environment since it helps to promote electronic healthcare records instead of using paper based records.
A5	Familiarity	Needs to be familiar with web application development, IPFS technology, blockchain technology, system security, and database management.

Chapter 8 Conclusions

8.1 Summary

The project aims to create a secure web application for managing patient medical records using ReactJS, NodeJS, Hyperledger Fabric, IPFS, and Keybase. The application will allow patients to have full control over their records and healthcare professionals to access them quickly. The application uses blockchain technology and IPFS for secure storage, with encrypted patient data stored in Keybase and accessed by doctors upon approval. The project requires expertise in various technologies, including ReactJS, NodeJS, Hyperledger Fabric, IPFS, cryptography, user interface design, security architecture, network security, software testing, deployment, and system administration.

8.2 Limitations

Due to the project's emphasis on security, it requires a significant amount of processing, which results in slower performance than a system that uses a traditional database server to store files. Additionally, the IPFS and blockchain technologies used in this project are relatively new, making it difficult to find relevant resources.

8.3 Future Improvement

Although this project uses tools that are currently considered to be the best, there are numerous scopes of improvement that can be made. As previously mentioned, the tools used provide excellent security, but at the cost of speed. In the future, these tools could be replaced with newer ones that offer faster performance. Additionally, the project currently relies on a third-party application to share encryption keys. In the future, it would be possible to develop a proprietary key sharing tool.Integrating the system to IoT devices and other fitness tracking devices can be also be viable and valuable for a certain group of users

References

1. Xia, Qi & Sifah, Emmanuel & Asamoah, Kwame & Gao, Jianbin & Du, Xiaojiang & Guizani, Mohsen. (2017). MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain. IEEE Access. PP. 1-1. 10.1109/ACCESS.2017.2730843.

2. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. *2016 2nd International Conference on Open and Big Data (OBD)*, 25-30.

3. Bowles, Juliana & Webber, Thais & Blackledge, Euan & Vermeulen, Andreas. (2021). A Blockchain-Based Healthcare Platform for Secure Personalized Data Sharing. 10.3233/SHTI210150.

4. Khan, Mohammad & Bourouis, Sami & Alsufyani, Abdulmajeed & Hasib, Kazi Tamzid Akhter. (2022). Electronic Health Record Monitoring System and Data SecurityUsing Blockchain Technology. Security and Communication Networks. 2022. 1-15. 10.1155/2022/2366632.