VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY
An Autonomous Institute Affiliated to University of Mumbai
Department of Computer Engineering

Project Report on

Aatmanirbhar Sanchar - Chat Application

In partial fulfilment of the Fourth Year, Bachelor of Engineering (B.E.) Degree in Computer Engineering at the University of Mumbai Academic Year 2023-24

Submitted by
Hitakrit Goplani - D17A/19
Shruti Dalvi - D17A/12
Swara Nabar - D17A/47
Krish Mehta - D17B/42

Project Mentors
Mr. Richard Joseph
Ms. Yugchhaya Galphat

(2023-24)

VIVEKANAND EDUCATION SOCIETY'S INSTITUTE OF TECHNOLOGY
An Autonomous Institute Affiliated to University of Mumbai
Department of Computer Engineering

Certificate

This is to certify that ***Hitakrit Goplani (D17A/19), Shruti Dalvi (D17A/12), Swara Nabar(D17A/47), Krish Mehta (D17A/42)*** of Fourth Year Computer Engineering studying under the University of Mumbai have satisfactorily completed the project on "***Aatmanirbhar Sanchar - Chat Application***" as a part of their coursework of PROJECT-II for Semester-VIII under the guidance of their mentor ***Mr. Richard Joseph and Ms. Yugchhaya Galphat*** in the year 2023-24 .

This project report entitled ***Aatmanirbhar Sanchar - Chat Application*** by ***Hitakrit Goplani, Shruti Dalvi, Swara Nabar, Krish Mehta*** is approved for the degree of ***B.E. Computer Engineering***.

Programme Outcomes	Grade
PO1,PO2,PO3,PO4,PO5,PO6,PO7, PO8, PO9, PO10, PO11, PO12 PSO1, PSO2	

Date:
Project Guide:

Mr. Richard Joseph Ms. Yugchhaya Galphat

टाटा मूलभूत अनुसंधान संस्थान
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
होमी भाभा रोड, कोलाबा, मुंबई – ४०० ००५.
Homi Bhabha Road, Colaba, Mumbai - 400 005.
परमाणु ऊर्जा विभाग की स्वायत्त संस्था
भारत सरकार एवं समविश्वविद्यालय
An Autonomonus Institution of the Department of Atomic Energy
Government of India and Deemed University

दूरभाष / Telephone : +91 22 2278 2000
फैक्स / Fax : +91 22 2280 4610 / 11
वेबसाईट / Website : www.tifr.res.in

Date: 05/8/2023

Letter of Permission

This is to certify that following Final year students of Department of Computer Engineering of Vivekanand Education Society's Institute of Technology, Chembur, are working on a TIFR project titled "**Data Security using Blockchain**", under the guidance of **Mrs. Yugchhaya Dhote and Mr. Richard Joseph** for the academic year 2023-24.

1. **Hitakrit Goplani**
2. **Shruti Dalvi**
3. **Swara Nabar**
4. **Krish Mehta**

We will provide all technical assistance to students required during the completion of the project. The progress seminars and meetings will be regularly conducted to take feedback.

Dr. Shashikant Dugad,

Professor, Department of High energy Physics,

Tata Institute of Fundamental Research, Mumbai.

Project Report Approval
For
B. E (Computer Engineering)

This project report entitled ***Aatmanirbhar Sanchar - Chat Application*** by ***Hitakrit Goplani, Shruti Dalvi, Swara Nabar, Krish Mehta*** is approved for the degree of ***B.E. Computer Engineering***.

Internal Examiner

External Examiner

Head of the Department

Principal

Date:
Place:

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

---------- ----------

(Hitakrit Goplani - D17A/19) (Shruti Dalvi - D17A/12)

---------- ----------

(Swara Nabar - D17A/47) (Krish Mehta - D17A/42)

Date:

ACKNOWLEDGEMENT

We are thankful to our college Vivekanand Education Society's Institute of Technology for considering our project and extending help at all stages needed during our work of collecting information regarding the project.

It gives us immense pleasure to express our deep and sincere gratitude to the Assistant Professor **Mr. Richard Joseph** and Professor **Mrs. Yugchhaya Galphat** (Project Guide) for her kind help and valuable advice during the development of project synopsis and for her guidance and suggestions.

We are deeply indebted to the Head of the Computer Department **Dr. (Mrs.) Nupur Giri** and our Principal **Dr. (Mrs.) J.M. Nair ,** for giving us this valuable opportunity to do this project.

We express our hearty thanks to them for their assistance without which it would have been difficult in finishing this project synopsis and project review successfully.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement several times.

Computer Engineering Department

COURSE OUTCOMES FOR B.E PROJECT

Learners will be,

Course Outcome	Description of the Course Outcome
CO1	Able to apply the relevant engineering concepts, knowledge and skills towards the project.
CO2	Able to identify, formulate and interpret the various relevant research papers and to determine the problem.
CO3	Able to apply the engineering concepts towards designing solutions for the problem.
CO4	Able to interpret the data and datasets to be utilised.
CO5	Able to create, select and apply appropriate technologies, techniques, resources and tools for the project.
CO6	Able to apply ethical, professional policies and principles towards societal, environmental, safety and cultural benefit.
CO7	Able to function effectively as an individual, and as a member of a team, allocating roles with clear lines of responsibility and accountability.
CO8	Able to write effective reports, design documents and make effective presentations.
CO9	Able to apply engineering and management principles to the project as a team member.
CO10	Able to apply the project domain knowledge to sharpen one's competency.

CO11	Able to develop a professional, presentational, balanced and structured approach towards project development.
CO12	Able to adopt skills, languages, environment and platforms for creating innovative solutions for the project.

Index

List of Figures

List of Tables

Abstract

Amid growing concerns regarding digital privacy and security, the development of a chat room application takes on heightened importance. This innovative project introduces a decentralised and highly secure communication platform, seamlessly integrating blockchain technology to effectively tackle challenges related to authentication, end to end encryption, and data storage. Users gain the ability to establish chat rooms and engage in secure conversations, facilitated by Hyperledger fabric that oversees user authentication, chat room particulars, and message preservation. The bedrock of this system centres around the issuance of authentication, ensuring robust user verification prior to access. Notably, the entire user journey – spanning authentication to messaging – is meticulously recorded on an immutable blockchain ledger, amplifying transparency and circumventing the need for central intermediaries. The proposed solution makes smart use of blockchain's benefits, creating a world where communication is trustworthy, private, and super secure.

Chapter 1: Introduction

1.1 Introduction

The advent of digital communication has revolutionised the way people interact and share information. According to the data provided by 'Statistic.com', as depicted in Figure 1, as of January 2024, WhatsApp boasted a monthly user base of two billion, with particularly robust penetration in markets beyond the United States, solidifying its position as one of the most widely used mobile social apps worldwide. WeChat amassed over 1.3 billion users, while Facebook Messenger recorded approximately 980 million users globally. Instant messaging, characterized by real-time text transmission over the internet, has flourished with the advent of smartphones and the proliferation of mobile apps. These low-cost or free chat and social messaging platforms have emerged as cost-effective alternatives to traditional SMS-based text messaging provided by mobile operators. Offering an array of features such as group chats, multimedia exchange including graphics, video, and audio messages, as well as stickers or emoticons, these messenger apps have reshaped the landscape of digital communication.

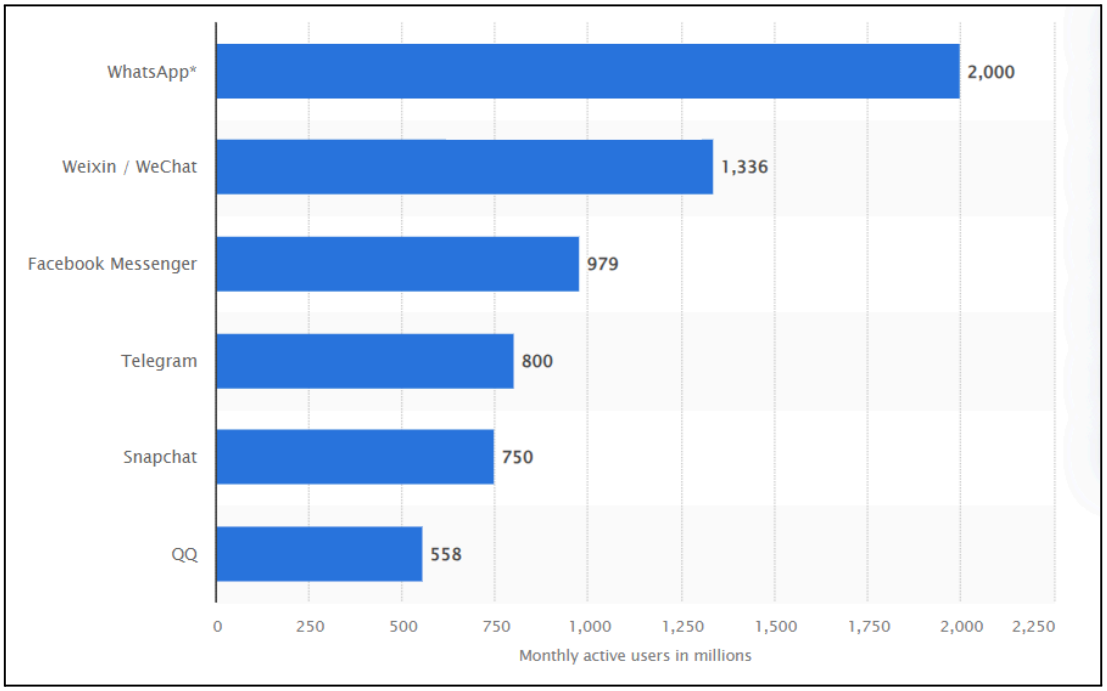

Figure 1.1 : Most popular global mobile messenger apps as of January 2024, based on number of monthly active users(in millions) Source: Statista

However, this convenience has brought forth a host of security and privacy concerns. Traditional chat applications often struggle to strike a balance between ease of use and safeguarding user data, resulting in vulnerabilities that threaten the confidentiality of conversations. This project aims to tackle these challenges head-on by introducing a decentralized chat room application that capitalizes on the robust capabilities of blockchain technology. Central to this solution is the amalgamation of secure authentication and tamper-proof storage through the application of blockchain. The decentralized nature of blockchain eliminates the need for centralized authorities, fostering an environment of trust and privacy. All this is done to not only validate user identities but also governs chat room details and key generation. Upon successful authentication, users gain entry into the chat room, where encryption safeguards the content of their conversations. Messages exchanged within this secure enclave are encrypted using keys generated by the crypto material generated for individual users Upon logout, the conversation details are securely stored in individual blocks within the blockchain ledger for different chat rooms. This immutable record guarantees the integrity and authenticity of messages, providing a high level of transparency and auditability. Through this approach, the proposed solution not only addresses the existing pitfalls of mainstream chat applications but also charts a course toward a more secure, private, and trustworthy digital communication landscape.

1.2 Motivation

The motivation for implementing a remote access control system to sensitive areas using crypto cards is rooted in the fundamental need to enhance security, streamline access management, and safeguard critical assets, reducing human error, improving access control, enhancing auditability and accountability, cost efficiency, scalability, leveraging technological advancements, deterring unauthorised access, and protecting sensitive data. Crypto cards offer a more secure and tamper-resistant means of verifying a user's identity, providing a robust audit trail, and reducing the need for frequent reissue of access credentials. They also offer cost savings compared to traditional key-based systems, making them a cost-effective solution for organizations growing or evolving. The project aims to establish a robust and efficient means of controlling access to sensitive areas, ultimately safeguarding critical assets and information.

1.3 Problem Definition

The problem at hand revolves around the existing limitations and vulnerabilities inherent in mainstream chat applications. While these platforms offer a plethora of features and functionalities, including Voice Over Internet Protocol (VoIP), multimedia support, and end-to-end encryption, concerns persist regarding data privacy and security. Mainstream chat application's closed-source code raises doubts about the extent to which user information is safeguarded from unauthorized access and exploitation. Moreover, the absence of transparency regarding data handling practices leaves users vulnerable to potential data mining and privacy breaches. Therefore, there is a pressing need to address these shortcomings and develop a solution that prioritizes user privacy, security, and trust in the digital communication landscape. This research endeavors to explore the feasibility and efficacy of implementing a decentralized chat application using blockchain technology as a means to mitigate these concerns and provide users with a more secure and trustworthy communication platform.

1.4 Existing Systems

Traditional chat applications rely on centralized servers, leaving user data vulnerable to hacking and surveillance. In contrast, blockchain-based chat apps leverage decentralized networks, where messages are encrypted, stored securely across multiple nodes, and cannot be altered or censored. This ensures privacy, as users have full control over their data without the risk of third-party interference. Additionally, blockchain technology fosters trust through transparent and immutable transaction records, eliminating doubts about message integrity or manipulation.

1.5 Lacuna of the Existing Systems

1. Limited Adoption: Low user adoption due to preference for established platforms.
2. Scalability Issues: Slow message processing on some blockchain networks, impacting user experience.
3. Costs and Fees: Transaction fees can be a barrier, especially for frequent messaging.
4. Integration Difficulty: Challenging integration with existing systems limits usability

1.6 Relevance of the Project

Aatmanirbhar Sanchar, our innovative project, harnesses the power of blockchain technology to revolutionize communication in the digital era. By integrating decentralized and immutable features, our chat application ensures unparalleled security and transparency. Through encrypted messaging and decentralized storage, users can communicate with confidence, knowing that their data is protected from unauthorized access and manipulation. Aatmanirbhar Sanchar prioritizes user privacy by eliminating the need for third-party intermediaries, placing control firmly in the hands of the users themselves. With transparent transaction records and resistance to censorship, our platform fosters trust among users, paving the way for a more secure and self-reliant communication ecosystem. Join us in embracing the future of communication with Aatmanirbhar Sanchar.

Chapter 2: Literature Survey

A. Brief Overview of Literature Survey

A literature survey is a thorough summary of earlier studies on a subject. The literature survey examines scholarly books, journals, and other sources that are pertinent to a particular field of study. With respect to the proposed work, the literature survey comprises a number of research papers and various articles that were referred to during the study of the project. It also comprises Interaction with Industry Experts of Tata Institute of Fundamental Research (TIFR). The details of the same are mentioned below.

B. Related Works

2.1 Research Papers Referred

1. **Title:** Decentralized ChatApplication using Blockchain Technology, Keshav Khalkar et al. “Decentralized ChatApplication using Blockchain Technology”, JETIR, Volume 10, Issue 5, May 2023. Available at: https://www.jetir.org/papers/JETIR2305B41.pdf

    a. **Abstract:** Decentralised applications make use of peer-to-peer networks, this ensures that no network failure can occur due to central node failure .This project aims to develop a decentralised chat application using blockchain technology. The application leverages the decentralised and transparent nature of blockchain to provide users with a secure and user-controlled communication platform. The use of cryptographic techniques ensures message integrity and confidentiality, allowing users to exchange messages in a secure manner. Smart contracts deployed on the blockchain enable advanced functionalities such as automated moderation, reputation systems, and decentralised file storage. The project focuses on user adoption and interface design to provide a seamless and intuitive user experience. By harnessing the power of blockchain, the decentralised chat application offers enhanced privacy, security, and control over communication activities in the digital realm.

b. **Inference:** Keshav and Khalkar (2023) advocate for the adoption of decentralised chat applications, emphasising the need to move away from reliance on centralised servers [1]. Their proposal leverages blockchain technology to establish peer-to-peer networks and consensus mechanisms, thereby enhancing the stability and security of communication channels. This decentralised approach not only mitigates the risks associated with single points of failure but also fosters trust and transparency among users.

2. **Title:** BlockChain Based Chat Application, I. Lokhande, N. Deotale, B. Mali, S. Chauhan and J. Dhuri, "BlockChain Based Chat Application, " 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-6, doi: 10.1109/INCET57972.2023.10170739.
Available at: https://ieeexplore.ieee.org/document/10170739

a. **Abstract :** Peer-to-peer networks are used by decentralized applications to ensure that no network failure can be caused by a failing central node. Today's environment, where holding data on a centralized server might be unsafe and expensive, requires a decentralized application for communication and resource sharing. We developed a programme that uses blockchain technology and decentralized networks to guarantee user privacy and make it simple for blockchain administrators to track down the source of false rumors that circulate throughout the network. The workload for file synchronization and sharing is distributed among a service, a client and a provider. This paper focuses on how decentralization could assist in successfully overcoming such problems. Decentralization would result in an increase in workers who will transfer data from a client node to a server node. When sharing data, blockchain would guarantee security. The suggested model can be utilized to move large data in a comparatively faster time frame. Additionally, the study elaborates on the design implications and factors, a user must comprehend in order to use this model properly and to obtain better outcomes when deployed onto the systems.

b. **Inference:** The paper introduces a blockchain-based chat application aimed at enhancing user privacy and combating the spread of misinformation. By

integrating blockchain into the communication framework, their solution ensures secure and tamper-proof storage of messages, while also providing mechanisms for efficient data handling. This emphasis on privacy and data integrity aligns with the growing demand for secure communication channels in an increasingly digital world.

3. **Title:** Aatmanirbhar Sanchar: Self-Sufficient Communications, Jay Ravi Jhaveri, Prem Vinod Chabbria, Neeraj Narain Ochani, Abhay Anupam Gupta, Dr. Sharmila Sengupta, Prof. Sunita Suralkar, Prof. Shashi Dugad, "Aatmanirbhar Sanchar: Self-Sufficient Communications" . In: Hemanth, J., Pelusi, D., Chen, J.IZ. (eds) Intelligent Cyber Physical Systems and Internet of Things. ICoICI 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 3. Springer, Cham. https://doi.org/10.1007/978-3-031-18497-0_41 Available at : https://link.springer.com/chapter/10.1007/978-3-031-18497-0_41

   a. **Abstract:** In the light of recent war crimes and data piracy conspiracies, privacy is of utmost importance to an organization and even to an individual. The majority of the population is dependent on third-party services for their daily communication. Albeit these major corporations advertise "secure" means of chat transfer, they install various kinds of backdoors to sell the user's data to advertisers. Under the notion of going "Aatmanirbhar" i.e., Make in India, we have developed an indie solution without incorporating any third-party services or APIs. "Aatmanirbhar Sanchar" aims at providing users with a real-time off-the-grid, secure, and anonymous messaging service. It features an End-to-End encrypted transmission of messages and data files likewise. This is achieved by combining the open-source AES algorithm with a self-developed XOR encryption process.

   b. **Inference:** The paper proposes a novel approach to secure communication through an ephemeral chat application. By employing advanced encryption techniques such as XOR encryption, AES-256, and HMAC verification, the application ensures end-to-end security and integrity of transmitted messages and files. Furthermore, it explores the implications of such technology in diverse contexts, ranging from organizational communications to national

security concerns, advocating for a self-reliant approach in developing secure communication platforms. The paper concludes by emphasizing the significance of secure and private communication in the contemporary digital landscape and presents "Aatmanirbhar Sanchar" as a viable solution, hosted on private servers without external surveillance, offering users a platform for confidential communication.

4. **Title:** IPFS-Blockchain-Based Authenticity of Online Publications. Nizamuddin, Nishara & Hasan, Haya & Salah, Khaled. (2018). "IPFS-Blockchain-Based Authenticity of Online Publications", 10.1007/978-3-319-94478-4_14. Available at : https://www.researchgate.net/publication/325899234_IPFS-Blockchain-Based_Authenticity_of_Online_Publications

   a. **Abstract:** In this paper, we propose a solution to provide originality and authenticity of published and posted freely online digital content such as books, music, and movies. Our solution utilises a blend of newly emerging technologies that primary include (InterPlanetary File System) IPFS and blockchain smart con-tracts. IPFS is used to store digital content with a high integrity and global acces-sibility to all, and Ethereum smart contract is used to govern, manage, and provide traceability and visibility into the history of digital content from its origin to the latest version, in a manner that is decentralized and globally accessed with high integrity, resiliency, and transparency. In the paper, our solution is focused on online book publication, but the solution can be a framework that can be easily extendible and adoptable for, to other digital and multimedia content. The full code of our smart contract is provided, with discussion on implementation and testing of its key functionalities.

   b. **Inference:** The research paper [17] explores the integration of InterPlanetary File System (IPFS) and blockchain technology to establish a robust mechanism for verifying the authenticity of online publications. Through a meticulous investigation, it outlines the architecture and functioning of the combined IPFS-blockchain framework, elucidating how IPFS's decentralised file storage system and blockchain's immutable ledger are leveraged to ensure the integrity and authenticity of digital publications. The paper delves into the

process of timestamping publications on the blockchain and linking them to their corresponding files stored on IPFS, thus enabling transparent and tamper-proof verification of content authenticity. By presenting use cases and scenarios, the paper underscores the potential of this hybrid approach in mitigating issues related to misinformation, content tampering, and plagiarism in online publishing.

5. **Title:** Anonymous De-centralized Ephemeral Chat Application using Interplanetary File System, Khan, Faraz & Mantri, Niraj & Rajput, Sagar & Dhakane, Dhananjay & Padiya, Puja. (2020). "Anonymous De-centralized Ephemeral Chat Application using Interplanetary File System.", ITM Web of Conferences. 32. 02004. 10.1051/itmconf/20203202004. Available at : https://www.itm-conferences.org/articles/itmconf/pdf/2020/02/itmconf_icacc2020_02004.pdf

   a. **Abstract:** Communication is essential for human beings and we communicate globally with the means of internet every day. Internet is an interconnected mesh of networks where our data is transferred through hundreds of nodes before reaching its destination. As the intermediary network node increases, the risk of losing confidentiality and integrity is also affected. Decentralized Chat (DChat) is a chat service on the Interplanetary File System (IPFS) peer-to-peer protocol where users can communicate with ephemeral chats under any anonymous alias. The users are not aware of real identity of each other and the chats are lost from the service once the node is disconnected. The data is tamper-resistant because to alter it would change the hash and invalidate it from the network. Here we aim to develop a secure chat service that provides anonymity and ephemeral chats using cost-effective IPFS technology.

   b. **Inference:** The research paper discusses the development of a decentralized and anonymous chat application using Interplanetary File System (IPFS) technology to ensure privacy and security in online communications. By leveraging IPFS, the proposed chat system allows users to communicate anonymously under pseudonyms, with messages being ephemeral and automatically deleted upon disconnection. This approach addresses concerns

about electronic traces left by conventional centralized chat platforms like WhatsApp and Facebook, emphasizing the importance of privacy, integrity, and availability in online interactions. The study emphasizes the potential of IPFS for decentralized communication systems and underscores the benefits of ephemeral messaging for protecting user privacy in digital environments.

6. **Title:** Blockchain Technology: Applications, Benefits and Challenges, N. Baygin, M. Baygin and M. Karakose, "Blockchain Technology: Applications, Benefits and Challenges," 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, 2019, pp. 1-5, doi: 10.1109/UBMYK48245.2019.8965565. Available at : https://ieeexplore.ieee.org/document/8965565

    a. **Abstract:** Blockchain is the name given to the technology that allows any data set to be stored in a distributed manner. It provides a secure structure with its distributed structure and provides a transparent system with the data set easily accessible by each user. Bitcoin application using blockchain infrastructure has gained attention with its reliability, robustness and performance. Thus, the blockchain is provided to reach large masses. Although the blockchain stands out as the technology of the future, it presents several disadvantages according to the application fields. In this study, blockchains performed on application basis were compared. The advantages and disadvantages of this system, which is called the technology of the future, are examined and compared in detail.
    b. **Inference:** Blockchain decentralized, secure data storage has revolutionized financial transactions, but it's essential to understand that it has its drawbacks. This paper evaluates blockchain implementations in different applications to provide a comprehensive view of its advantages and disadvantages.

7. **Title:** BONIK: A Blockchain Empowered Chatbot for Financial Transactions, M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque and S. Tarkoma, "BONIK: A Blockchain Empowered Chatbot for Financial Transactions," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp.

1079-1088, doi: 10.1109/TrustCom50675.2020.00143. Available at : https://ieeexplore.ieee.org/document/9343092

a. **Abstract:** A Chatbot is a popular platform to enable users to interact with a software or website to gather information or execute actions in an automated fashion. In recent years, chatbots are being used for executing financial transactions, however, there are a number of security issues, such as secure authentication, data integrity, system availability and transparency, that must be carefully handled for their wide-scale adoption. Recently, the blockchain technology, with a number of security advantages, has emerged as one of the foundational technologies with the potential to disrupt a number of application domains, particularly in the financial sector. In this paper, we forward the idea of integrating a chatbot with blockchain technology in the view to improve the security issues in financial chatbots. More specifically, we present BONIK, a blockchain empowered chatbot for financial transactions, and discuss its architecture and design choices. Furthermore, we explore the developed Proof-of-Concept (PoC), evaluate its performance, analyse how different security and privacy issues are mitigated using BONIK.

b. **Inference:** The paper proposes the integration of blockchain technology, exemplified by "BONIK," to enhance the security of financial transactions in chatbots, addressing recognized security concerns in this context. Through careful design and a Proof-of-Concept demonstration, BONIK effectively mitigates security and privacy issues, showcasing the broader potential of blockchain in the financial sector.

8. **Title:** Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application, Fauziah, Noveline & Rachmawanto, Eko & Setiadi, De Rosal Ignatius Moses & Sari, Atika. (2018). "Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application" 146-151. 10.1109/ISRITI.2018.8864485. Available at :

https://www.researchgate.net/publication/336559998_Design_and_Implementation_of_AES_and_SHA-256_Cryptography_for_Securing_Multimedia_File_over_Android_Chat_Application

a. **Abstract:** In the current era of globalization, security is one of the most important aspects in the development of communication applications, especially when sending confidential files. Advanced Encryption Standard (AES) is one method that can be used to secure data by encrypting and decrypting an information. AES is also an algorithm that has a fast encryption process and has been widely implemented in various fields. To provide data security that is transferred to the network, AES is considered a fast and best algorithm. AES is an open source cryptography with symmetric keys used for encryption and decryption of files. Files to be encrypted are multimedia files such as images, audio and video. The file is entered into the application, then the user inputs a key that is encrypted with the SHA-256 algorithm to secure the contents of the file. Encrypted files are stored in the UUencoding format to avoid the compression process when sending files via the chat application. The file is also safer, because the message cannot be seen directly. Based on the results of experiments in this study, multimedia file encryption applications have been successfully built. Although the process of encryption and decryption changes the size of the original file a little, the contents and meaning of the file remain the same and has been wrapped up by measuring the PNSR value that produces an infinity value.

b. **Inference:** The research paper discusses the successful implementation of an Android application utilizing AES encryption with SHA-256 keys to securely encrypt and decrypt multimedia files such as images, audio, and video. The encryption process converts files into .enc format, ensuring secure transmission via messaging applications like WhatsApp. Despite a slight increase in file size due to encryption, the study demonstrates that the content remains unchanged, as verified by the PSNR (Peak Signal-to-Noise Ratio) analysis resulting in an infinity value. This confirms that the original content integrity is maintained throughout the encryption and decryption processes, enhancing data security for multimedia file transfers.

9. **Title:** Multihop Concurrent Big Data Sharing via Multithreading using Blockchain on a Decentralized Network, R. Bhatangar and V. B. Lobo, "Multihop Concurrent Big Data Sharing via Multithreading using Blockchain on a Decentralized Network," 2020 2nd International Conference on Advances in Computing, Communication Control

and Networking (ICACCCN), Greater Noida, India, 2020, pp. 885-890, doi: 10.1109/ICACCCN51052.2020.9362977. Available at : https://ieeexplore.ieee.org/document/9362977

a. **Abstract:** This study aims to provide a novel concept of multihop concurrent communication between blockchain network peers to facilitate big data sharing via threads in a multithreaded environment to reduce effective transmission time required for sharing a large file. In a general client-server model, the entire load of sharing and synchronization of files is split among a service provider and a client. A three-tier model too provides the same rate of speed irrespective of the number of nodes a current node is connected with, provided there is no network congestion. This paper focuses on how decentralization might help to effectively overcome such problems. Decentralization would increase the number of workers that will redirect data from a server node to a client node and blockchain would maintain security when data is being shared. The proposed model can be used to transfer big files in a relatively less span of time. Moreover, the study elaborates on design implications and considerations a user must understand to effectively use this model for achieving the holy grail to acquire better results when implemented on his/her systems.
b. **Inference:** The research paper explores a novel approach for achieving efficient and secure multihop concurrent big data sharing through multithreading and blockchain technology on a decentralized network. By leveraging multithreading techniques, the system can handle concurrent data transactions effectively, enhancing throughput and scalability in big data sharing scenarios. Integrating blockchain ensures data integrity, transparency, and security across multiple hops within the decentralized network. This innovative solution addresses key challenges in decentralized data sharing, offering a promising direction for future developments in distributed computing and blockchain applications.

10. **Title:** Securing Medical Forensic System Using Hyperledger Based Private Blockchain, M. Ahmed, S. Reno, N. Akter and F. Haque, "Securing Medical Forensic System Using Hyperledger Based Private Blockchain," 2020 23rd International

Conference on Computer and Information Technology (ICCIT), DHAKA, Bangladesh, 2020, pp. 1-6, doi: 10.1109/ICCIT51783.2020.9392686. Available at : https://ieeexplore.ieee.org/document/9392686

a. **Abstract:** Forensic pathology applies medical skills and knowledge to a criminal inquiry that recognizes or develops the information regarding the accidental or unlawful death of an innocent person or the victims of significant physical injury. It is a legal process which collects, examines, analyzes and reports the evidence. Hyperledger Fabric is a permissioned and private blockchain structure which includes the present estimation of the element's property and the historical backdrop of transactions. In forensic department, every piece of evidence should be properly identified, collected, preserved, analyzed and finally admitted to the proper authority. But in reality assembling, evaluating, storing evidence is not secured enough. So in this paper, we are focused on creating a blockchain based medical forensic system using Hyperledger. The system can track any unauthorized access and modification by retrieving the Historian Record and Asset Registries and thus guarantees the impartiality of evidence, secrecy and validity of transactions.
b. **Inference:** The research paper proposes a secure medical forensic system using a private blockchain based on Hyperledger technology. By leveraging Hyperledger's private and permissioned blockchain framework, the system ensures confidentiality, integrity, and traceability of medical forensic data. This approach addresses the critical need for secure and tamper-proof storage and sharing of sensitive medical information, enhancing trust and accountability in forensic investigations. The use of private blockchain ensures controlled access to data among authorized participants, safeguarding patient privacy and regulatory compliance. Overall, the study demonstrates the potential of blockchain technology in enhancing security and transparency in medical forensic systems.

2.2.Books/ Journals/ Articles referred

Books:

1. "Mastering Bitcoin" by Andreas M. Antonopoulos: This book provides a comprehensive understanding of Bitcoin and blockchain technology, which can be foundational for your project.
2. "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher: This book offers a beginner-friendly introduction to blockchain concepts, which can help you grasp the fundamentals.
3. "Blockchain Applications: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti: This book covers various blockchain applications, including secure messaging, and can be useful for practical implementation.

Journals and Articles:

1. "Blockchain Technology: Principles and Applications" - This article, published in the International Journal of Research in Engineering and Technology, provides a comprehensive overview of blockchain technology and its potential applications.
2. "Blockchain and Its Use in Financial Settlement and Clearing" - This paper in the Journal of Financial Market Infrastructures discusses the use of blockchain in financial transactions, which may have relevance to your project.
3. "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology" - This article, published on Bitcoin Magazine, discusses the concept of decentralized applications and their potential.

2.3 Interaction with Industry Experts

As our project titled ‘Aatmanirbhar Sanchar - Chat Application’ is in collaboration with **‘Tata Institute of Fundamental Research’**, we had an opportunity to interact with Dr. Shashi Dugad who works at TIFR. He provided us with a clear insight of the project and guided us on how to start with the project. From then, after every two or three weeks, we had an interaction with Shashi sir, to show the implementation of what we had done. He evaluated our work and told us the further things we need to perform. Overall, Shashi sir acted like a guiding light for us.

2.4 Patent Search

1) **Patent No. US7739508B2**, granted by USPTO dated 2010-06-15 titled, “secure instant messaging system” provides practical insights into the implementation of blockchain principles for message security and privacy. It integrates secure text messaging and file transfers by providing users with security certificates from a certificate authority (CA) to encrypt and decrypt messages and files. By leveraging security certificates and encryption techniques, this patent exemplifies how blockchain can be utilized to enhance the confidentiality and integrity of digital communication.

2) **Patent No. US10505877B2**, published on UPSTO dated 2019-12-10, titled, “Messaging systems and methods that employ a blockchain to ensure integrity of message delivery” utilizes blockchain technology for message verification and integrity. The system involves multiple message servers and a distributed database storing a blockchain. When a message is received by the first message server from a user, certain components of the message are recorded into a blockchain block stored in the distributed database. This recording ensures that the message data is tamper-proof and can be verified by subsequent servers in the system. When the second message server receives messages, it checks whether specific components of the message match those recorded in the blockchain, thereby allowing for verification and validation of message integrity across the distributed messaging system. This system leverages blockchain's immutability and decentralized nature to enhance message security and reliability.

2.5 Inference Drawn

Based on the research papers and patents discussed, it is evident that there is a strong emphasis on leveraging advanced technologies such as blockchain, AES encryption, and decentralized networks to enhance security and integrity in various domains. The use of blockchain in messaging systems ensures message verification and tamper-proof records, enhancing overall system reliability. AES encryption is widely employed for secure file transmission, especially in communication applications handling confidential data. Furthermore, the integration of Hyperledger in medical forensic systems highlights the

growing interest in blockchain for maintaining privacy and security in sensitive data environments. These technologies collectively contribute to advancing secure communication, data sharing, and system integrity across diverse applications and industries.

2.6 Comparison with the Existing System

Existing Blockchain based chat applications	Our Proposed blockchain based chat application
Blockchain-based secure chat applications often required users to navigate through complex wallet setups and cryptographic keys, making them less user-friendly for non-technical users.	Our proposed solution focuses on providing a user-friendly chat application that simplifies the user experience, reducing the need for complex key management.
Lack of interoperability between different blockchain-based chat applications meant that users on one platform couldn't easily communicate with users on another blockchain-based chat platform, limiting the overall reach and effectiveness of these systems.	We plan to address the interoperability issue, allowing users on your platform to communicate with users on other blockchain-based chat systems.
Using blockchain networks for message storage and processing often incurred transaction fees, which could be a barrier for some users, especially for frequent messaging or microtransactions.	Our solution aims to use private blockchain that removes the transaction fees for messaging.
Verifying the identity of users in a decentralized manner while maintaining privacy was a complex challenge. Ensuring trust and security in user interactions remained a concern.	Our solution seeks innovative approaches for user identity verification while preserving user privacy by generating unique cryptographical identifiers and storing them in the ledger.

Table 2.1: Comparison with existing systems

Chapter 3: Requirement Gathering for the Proposed System

3.1 Introduction to requirement gathering

Requirement gathering is a critical phase in the software development lifecycle, encompassing the systematic gathering and documentation of stakeholders' needs, expectations, and constraints for a software project. This process involves engaging with various stakeholders, including clients, end-users, subject matter experts, and other relevant parties, to understand the purpose, scope, and objectives of the project. Techniques such as interviews, surveys, workshops, and observations are commonly employed to elicit requirements effectively. Additionally, documentation plays a vital role in capturing and organizing gathered requirements, ensuring clarity, traceability, and alignment with project goals. Successful requirement gathering lays the foundation for developing software solutions that meet stakeholders' needs, mitigate risks, and deliver value to the intended users.

The requirements for the project titled "Aatmanirbhar Sanchar - Chat Application" comprises of:

3.2 Functional Requirements

1. User Registration:
    a. The user registration process should collect essential information such as email, password, and name to create a unique user account.
    b. It should include validation checks to ensure that the email provided is unique and follows the correct format, and that the password meets security requirements such as minimum length and complexity.

2. Login/Authentication:
    a. Upon registration, users should be able to log in securely using their email and password credentials.
    b. The authentication process should employ robust security measures, such as encryption and hashing, to safeguard user credentials and prevent unauthorized access.
3. Personal Messaging:

a. Users should have the capability to initiate one-on-one conversations with another user, ensuring private and direct communication.
b. The personal messaging feature should include functionalities like sending text messages, multimedia files, and emojis.

4. Group messaging:
    a. The application should support group messaging functionality, allowing multiple users to participate in a single conversation.
    b. Users should be able to create, join chat rooms.

5. Private Ledger for each chat room:
    a. When a new chat room is created, the system should automatically generate a private ledger exclusively for that room to store conversation data securely.
    b. Each ledger should be accessible only to the members of the corresponding chat room, ensuring data privacy and integrity

6. Access control to join chat room
    a. When a user requests to join a chat room, the system should notify the group admin or moderator, who can then approve or reject the request.
    b. Access control mechanisms should be in place to manage membership within chat rooms, allowing admins to maintain the privacy and security of group conversations while enabling seamless user interaction.

3.3 Non-Functional Requirements

1. Security:
    a. The system must adhere to industry-standard security practices to prevent unauthorized access, data breaches, and tampering.
    b. Encryption and secure protocols should be used to protect data in transit and at rest.
2. Performance:
    a. The system should provide quick and responsive access control, ensuring minimal delays in granting or denying access.
    b. It should handle a high number of concurrent access requests efficiently.

3. Reliability:
    a. The system should have high availability to ensure continuous access control operations, even in the event of hardware or software failures.
    b. Backup and redundancy mechanisms should be in place.
4. Scalability:
    a. The system should be able to scale to accommodate an increasing number of users and access points without a significant decrease in performance.
5. Usability:
    a. User interfaces should be intuitive and user-friendly.
6. Maintenance:
    a. Regular maintenance and updates should be performed to address security vulnerabilities and system improvements.
    b. System downtime for maintenance should be minimized.
7. Cost-Effectiveness:
    a. The system should be designed and implemented in a cost-effective manner, considering both initial setup costs and ongoing operational expenses.

3.4 Hardware, Software, Tools and Techniques utilized

Hardware:

1. PC with Linux System

Software:

1. Web Development:
    a. Frontend Framework: ReactJS
    b. Backend Framework: NodeJS, ExpressJS
2. Blockchain:
    a. Hyperledger Fabric
    b. InterPlanetary File System (IPFS)
3. Operating System:
    a. Ubuntu (22.04)
    b. Windows 10/11

Tools:

1. VSCode

Techniques utilized till date for the proposed system :

1. **ReactJS**: Utilized for building the frontend interface, ReactJS offers a component-based architecture, enabling efficient UI development with reusable and modular components, enhancing user experience and interactivity.

2. **Node.js and Express.js**: Employed for backend development, Node.js provides a runtime environment for executing JavaScript on the server-side, while Express.js offers a lightweight web application framework. Together, they facilitate seamless server-side logic, routing, and API handling, ensuring robust and scalable backend functionality.

3. **Hyperledger Fabric:** Chosen for blockchain integration, Hyperledger Fabric provides a permissioned framework for developing enterprise-grade blockchain solutions. With features like private channels and smart contracts, it ensures secure and efficient transaction processing, fostering trust and transparency in data management.

4. **IPFS (InterPlanetary File System):** Integrated for decentralized file sharing on the blockchain, IPFS offers a distributed protocol for storing and sharing files across a peer-to-peer network. By leveraging IPFS, your project enables efficient and censorship-resistant file storage, enhancing data integrity and accessibility within the blockchain ecosystem.

3.5 Constraints

1. **For developers**
    a. PC should have Linux OS since Hyperledger works only on Linux

2. **For users**
    a. To access the application and use features of the application a good internet speed is required.

Chapter 4: Proposed Design

4.1 Block Diagram of the System

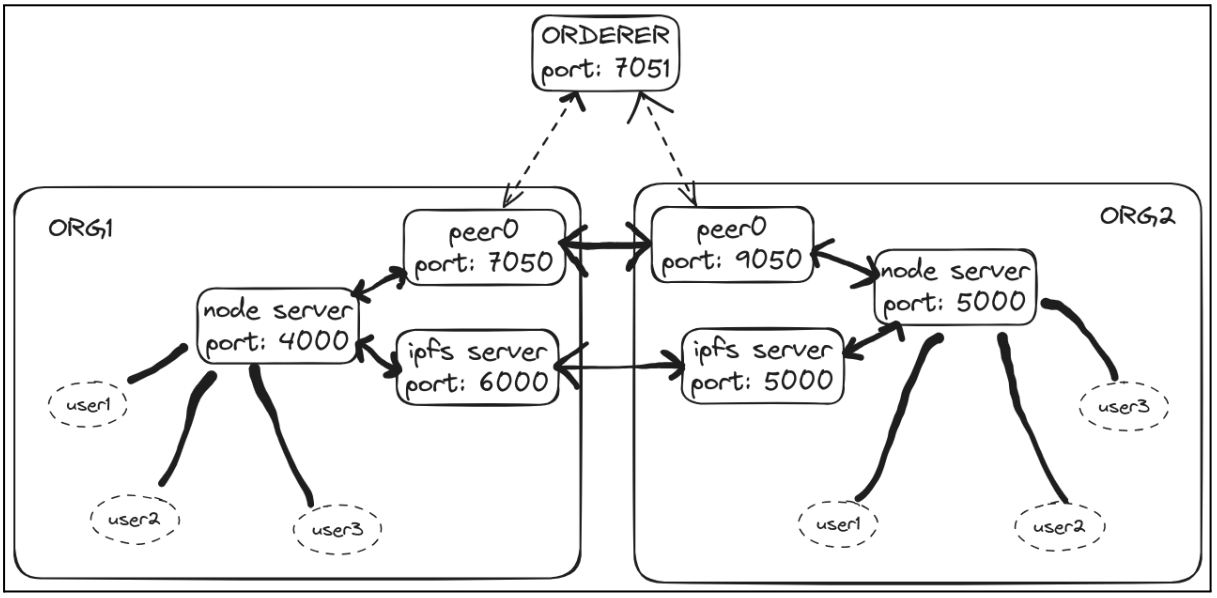

Figure 4.1: Block Diagram of the System

As shown in **figure 4.1** each organisation represents a distinct entity (e.g., a company, institution) within the Hyperledger Fabric network. Organisations maintain their own set of peer nodes and can interact with each other through shared channels and smart contracts. Peer nodes maintain the state of the ledger and participate in endorsing transactions (communication). The node server hosts the peer nodes and provides the necessary infrastructure for running the Hyperledger Fabric network. It manages the communication and interaction between different components of the network, including peer nodes, orderer nodes, and external services like IPFS. The IPFS (InterPlanetary File System) server is a decentralized storage system used for storing and sharing files and data within the network. The orderer node is responsible for maintaining the order of transactions and ensuring consensus across the network. In this diagram, a common orderer node is shared by both organizations (Org1 and Org2) to facilitate transaction ordering and block creation.

4.2 Modular design of the system

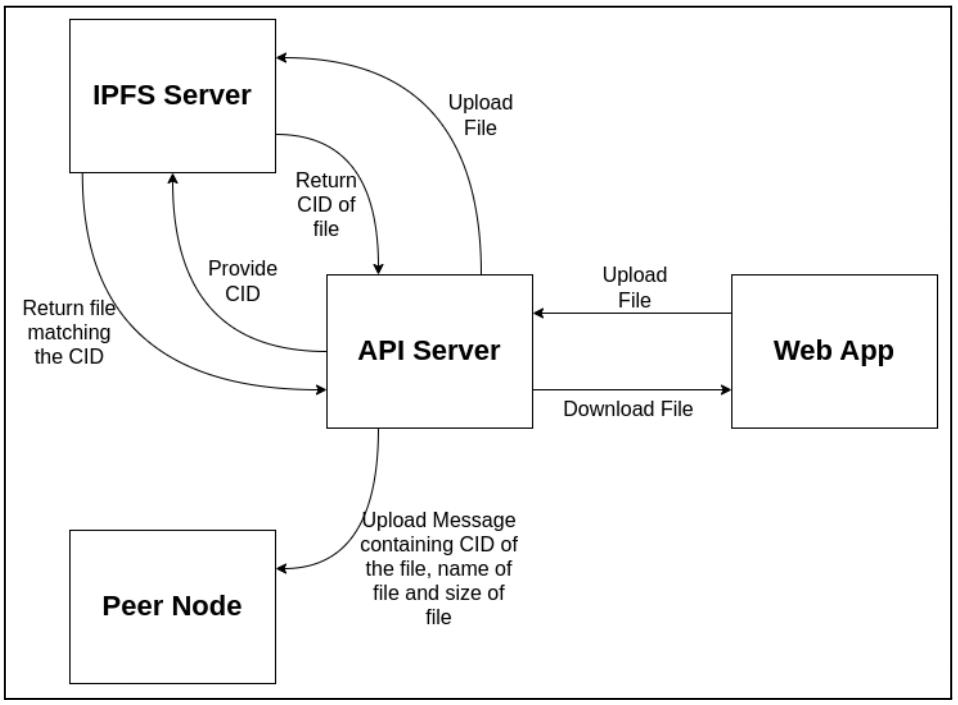

Figure 4.2: Modular design of the system

As shown in **figure 4.2**, the integration of Interplanetary File System (IPFS) enhances security and storage capabilities, ensuring secure and efficient handling of media files exchanged within the chat rooms:

1. Decentralized Data Transfer: IPFS operates as a decentralized protocol for content-addressed data transfer, ensuring that files are distributed across multiple nodes rather than centralized servers. When users exchange media files within the chat application, IPFS facilitates the transfer of data in a decentralized manner, enhancing security and resilience against single points of failure.
2. Fragmentation and Hashing: Before transmission, files are fragmented into smaller blocks to optimize data transfer and storage efficiency. Each block undergoes cryptographic hashing using the SHA-256 algorithm, ensuring that the integrity of the data is maintained throughout the transfer process. This fragmentation and hashing process enhances data integrity and tamper resistance, safeguarding the integrity of media files exchanged within the chat application.
3. Content Addressing: Each data block within IPFS is assigned a unique Content Identifier (CID) based on its content, rather than its location. This content addressing mechanism enables efficient retrieval and verification of media files, as users can

access files based on their unique identifiers regardless of their physical location within the network.

4. IPFS Kubo Implementation: IPFS daemon servers, deployed within the chat application's infrastructure, facilitate decentralized data storage and retrieval. These servers ensure that media files exchanged within the chat application are stored across multiple nodes, enhancing security and data availability. The implementation of IPFS Kubo enhances security by decentralizing data storage and retrieval, reducing reliance on centralized servers and mitigating the risk of data loss or unauthorized access.

4.3 Detailed Design

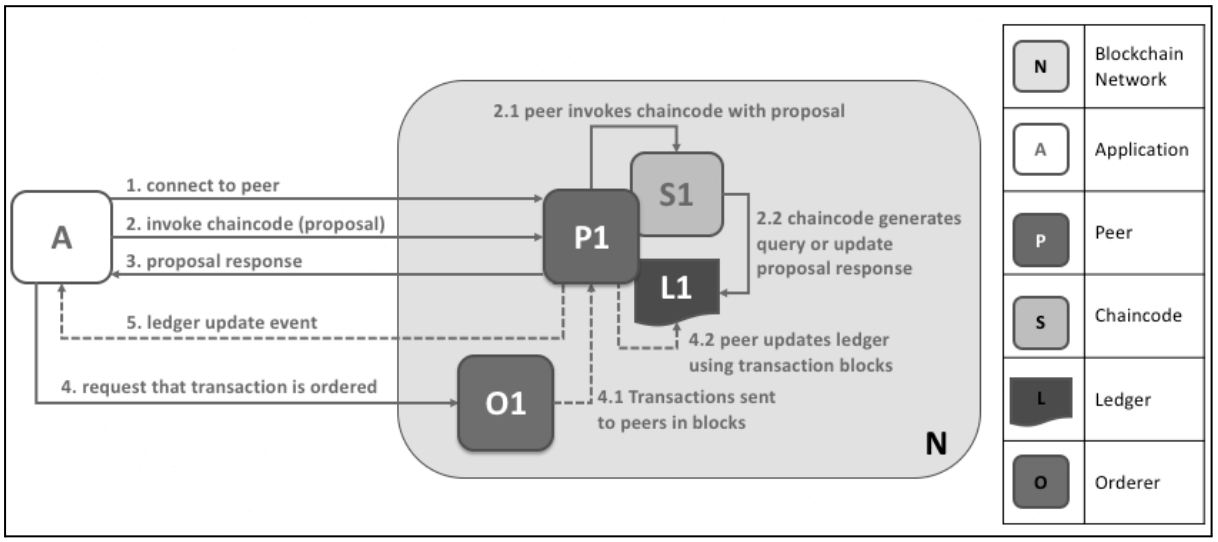

Figure 4.3: Types of Nodes

Types of nodes in Hyperledger Fabric

1. **Peer Node** : Every organization has to have at least one peer node. The peer node acts as an endpoint for users to communicate with the blockchain network. The peer node performs two actions
    a. **Endorsing**
        i. This involves taking a request from a user, validating it and sending this validated request to the orderer.
    b. **Committing**
        i. This involves taking the endorsed block from the orderer node and committing it to the blockchain network.

2. **Orderer Node :** A single orderer node can be used among multiple organizations. An orderer node takes endorsed requests from all the peer nodes and transforms them into blocks or assets that can be added to the blockchain ledger. This block is sent back to the peer node for committing.

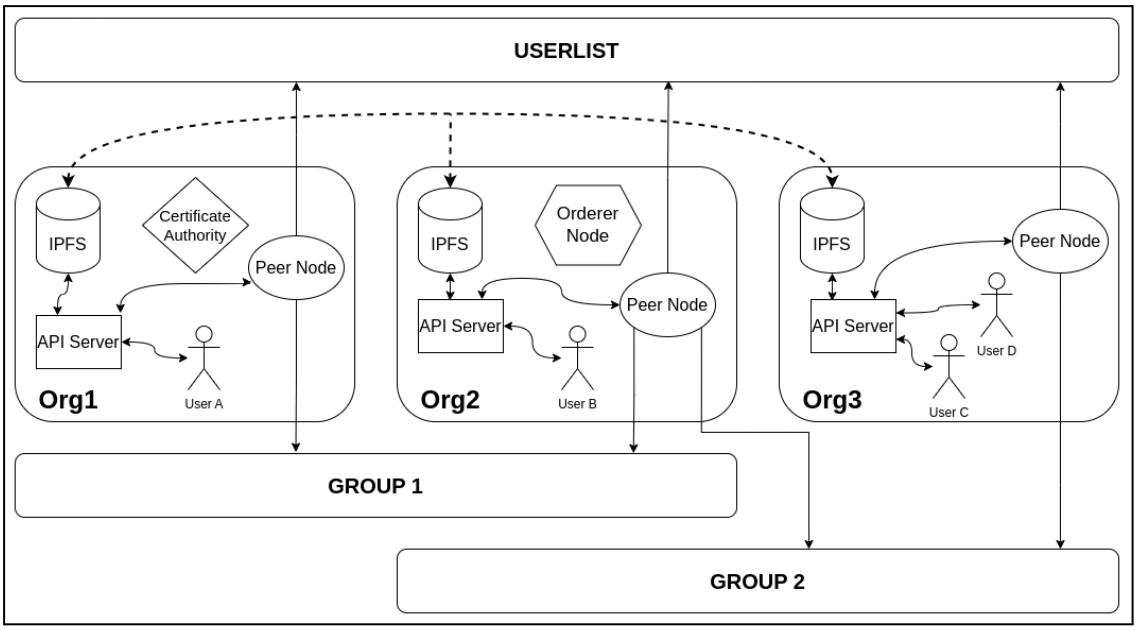

Figure 4.4: Detailed Design of the system

Figure 4.3 describes how Hyperledger Fabric plays a pivotal role in orchestrating various critical components, ensuring secure and confidential digital interactions:

1. Organization Setup: Within the application, organizations are established to represent different entities within the network, such as users or chat room administrators. Each organization is equipped with peer nodes responsible for transaction processing. These nodes serve as transaction endpoints, facilitating interactions with the ledger.
2. Transaction Processing: Peer nodes execute chaincode logic, which defines the permissible operations within the channels. For instance, when a user sends a message in a chat room, the chaincode governs the validation and recording of this transaction on the ledger. Consensus mechanisms, such as the Raft protocol, ensure agreement among network participants regarding the order and validity of transactions, enhancing the integrity of the ledger.
3. User Authentication: Certificate authorities issue digital certificates to users within the network, enabling secure communication and user authentication. These certificates

validate the identity of users and ensure that only authorized individuals can access and interact with the chat application.

4. Channel-based Segregation: Channels are employed to segregate communication into distinct groups or chat rooms, ensuring data privacy and confidentiality. Each channel has its ledger, which stores the transactions and interactions specific to that particular group, enhancing data segregation and privacy.
5. Chaincode: Chaincode defines the logic within the channels, dictating the permissible operations that users can perform. For example, the chaincode governs the creation of new chat rooms, joining or leaving existing ones, and the exchange of messages or media files within the chat application.

4.4 Project Scheduling & Tracking using Gantt Chart

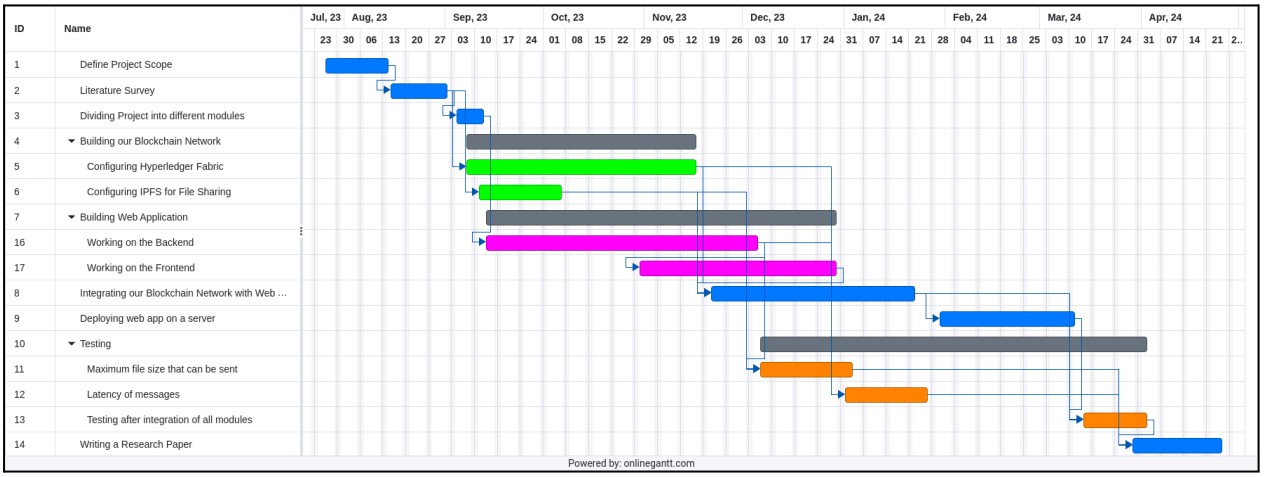

Figure 4.5: Gantt Chart

Chapter 5: Implementation of the Proposed System

5.1. Methodology employed for Development

Aatmanirbhar Sanchar operates to ensure secure and confidential communication among users.

1. Upon initiation, users are prompted to either log in or register, whereupon existing chat rooms and conversations are displayed on the home screen. The application employs a robust authentication mechanism to verify user identity and maintain data confidentiality.
2. The process of joining a chat room entails user requests, which are authenticated and processed by the respective chat room administrators.
3. Once granted access, users engage in secure communication facilitated by the blockchain network.
4. Text messages are transmitted directly, ensuring real-time interaction, while media files are securely uploaded to IPFS for decentralized storage and retrieval.

In this system, a web-based application serves as the user interface, allowing users to interact with the blockchain network. A server acts as an intermediary, receiving requests from the client application and facilitating communication with the blockchain network. The blockchain network itself is accessed through a dedicated API endpoint provided by a peer node within the network. This endpoint allows authorized users to initiate transactions. Aatmanirbhar Sanchar integrates Hyperledger Fabric (HLF) and Interplanetary File System (IPFS) to establish a robust framework for secure and confidential digital interactions.

5.2 Algorithms and Flowcharts for the Respective Modules developed

Elliptical Curve Digital Signing Algorithm (ECDSA)

Usage: Hyperledger Fabric CA employs ecdsa algorithms to sign digital certificates and transactions.

1. Elliptic Curve Cryptography (ECC):

At the heart of ECDSA is Elliptic Curve Cryptography, which utilizes the mathematics of elliptic curves over finite fields to provide security. Elliptic curves are algebraic structures defined by equations of the form: $y^2 = x^3 + ax + b$

In ECC, points on the curve can be added and multiplied, and this forms the basis of cryptographic operations.

2. Key Generation:

ECDSA relies on key pairs: a private key and a corresponding public key.

Private keys are randomly generated integers, usually chosen from a specific range defined by the curve's parameters.

Public keys are derived from the private keys using point multiplication. Specifically, a point on the elliptic curve is multiplied by the private key to obtain the corresponding public key.

3. Signing:

To sign a message using ECDSA, the signer:

1. Computes a message digest (hash) of the message to be signed using a cryptographic hash function (e.g., SHA-256).
2. Generates a random number k (called the nonce).
3. Computes a point R on the curve by multiplying the generator point G by k.
4. Derives the x-coordinate of R modulo the curve's order n.
5. Computes the value s such that $(k-1(z+rd)) \bmod n$, where z is the message digest, r is the x-coordinate of R, d is the signer's private key, and k^{-1} is the modular inverse of k modulo n.
6. The signature is the pair (r, s).

4. Verification:

To verify a signature, the verifier:

1. Recomputes the point R using the x-coordinate r from the signature.
2. Computes the message digest z of the message.
3. Computes $w = s^{-1} \bmod n$ and $u_1 = zw \bmod n$, $u_2 = rw \bmod n$.
4. Computes the point $X = u_1G + u_2Q$, where Q is the public key corresponding to the private key used to generate the signature.
5. If the x-coordinate of X is equal to r, the signature is valid; otherwise, it's invalid.

5. Security:

The security of ECDSA relies on the difficulty of the discrete logarithm problem in the context of elliptic curves, which states that given a point P and a multiple kP, it's computationally difficult to determine the integer k.

Secure Hash Algorithm 256-bit (SHA-256)

Usage: Hyperledger Fabric and IPFS use SHA-256 for hashing.

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function belonging to the SHA-2 (Secure Hash Algorithm 2) family. It is one of the most widely used hash functions and is employed in various security applications, including digital signatures, message integrity verification, password hashing, and blockchain technology.

1. Purpose:

SHA-256 generates a fixed-size (256-bit or 32-byte) hash value, regardless of the size of the input data. This hash value serves as a unique and compact representation of the input data.

The primary purpose of SHA-256 is to produce a digest (hash) of data in such a way that any change in the input data results in a significantly different hash value, making it suitable for ensuring data integrity and authenticity.

2. Algorithm:

SHA-256 operates on blocks of data, each 512 bits (64 bytes) in size. If the input data is not an exact multiple of 512 bits, it is padded to reach this length.

The algorithm consists of several rounds of processing, where each round applies a series of logical functions, bitwise operations, and permutations to the input data.

During each round, the algorithm processes a block of data and updates the internal state of the computation until the entire input data has been processed.

The final output of SHA-256 is a 256-bit hash value, typically represented as a 64-character hexadecimal string.

3. Properties:

Deterministic: For the same input data, SHA-256 always produces the same hash value. This property ensures reproducibility and consistency.

Pre-image Resistance: Given a hash value, it should be computationally infeasible to find the original input data. In other words, SHA-256 is resistant to pre-image attacks.
Collision Resistance: It is computationally infeasible to find two different inputs that produce the same hash value (collision). SHA-256 is designed to minimize the probability of collisions, making it suitable for cryptographic applications.
Avalanche Effect: A small change in the input data should produce a significantly different hash value. This property ensures that even minor alterations in the input data result in drastically different hash values.

4. Security:
SHA-256 is considered secure for most cryptographic applications and is widely used in practice. However, as computing power advances, cryptographic algorithms may become vulnerable to new attacks.
No significant vulnerabilities have been discovered in SHA-256 that would compromise its security or effectiveness for its intended purposes.

Practical Byzantine Fault Tolerance (PBFT)

Usage: Hyperledger Fabric uses PBFT for achieving consensus in the network

PBFT, or Practical Byzantine Fault Tolerance, is a consensus algorithm designed to achieve consensus in distributed systems, even in the presence of Byzantine faults. Byzantine faults refer to arbitrary or malicious behavior exhibited by nodes in a distributed system, such as sending contradictory messages, delaying messages, or acting in ways contrary to the protocol's rules. PBFT was introduced by Miguel Castro and Barbara Liskov in 1999.

1. Need for PBFT:
In a distributed system, nodes may fail or behave maliciously, leading to inconsistencies in the system's state. Traditional consensus algorithms like Paxos or Raft assume that the majority of nodes are honest. However, in some scenarios, these assumptions may not hold, particularly in permissioned or decentralized systems.
PBFT addresses the Byzantine Generals Problem, where a group of generals must agree on a coordinated action despite the presence of traitorous generals who may send conflicting messages.

2. Core Idea:

PBFT enables a set of nodes to agree on the order of transactions in a distributed system, even if some nodes are faulty or malicious. PBFT operates in a synchronous network model, where bounds on message delivery and processing times are known. This simplifies the algorithm's design but may limit its applicability in certain real-world scenarios.

3. Algorithm Overview:

PBFT involves a set of nodes, typically referred to as replicas, which communicate and reach a consensus on the order of transactions.

The algorithm proceeds through several phases:

1. Request: A client sends a request to the replicas.
2. Pre-Prepare: The primary replica assigns a sequence number to the request, creates a digest of the request, and sends a pre-prepare message to all other replicas.
3. Prepare: Upon receiving a pre-prepare message, each replica validates the message, creates a prepare message, and sends it to all other replicas.
4. Commit: Once a replica receives prepare messages from a two-thirds majority of replicas (including itself), it sends a commit message to all other replicas.
5. Execute: After receiving commit messages from a two-thirds majority, a replica executes the request, sends a response to the client, and broadcasts the response to all other replicas.

Replicas exchange messages in a peer-to-peer manner, and each replica maintains a state machine to track the sequence of executed requests.

4. Properties:

Safety: PBFT guarantees safety by ensuring that honest replicas agree on the order of transactions and the state of the system.

Liveness: The algorithm ensures liveness by continually making progress as long as the majority of replicas are honest and the network operates within expected bounds.

Tolerance: PBFT can tolerate up to one-third of the replicas being Byzantine faulty while still maintaining safety and liveness properties.

5. Applications:

PBFT is commonly used in permissioned blockchain networks, consortium blockchains, and distributed databases where a known set of nodes need to agree on the order of transactions while tolerating Byzantine faults. It's used in systems requiring strong consistency guarantees, such as financial systems, supply chain management, and distributed ledgers for enterprise applications.

Flowchart:

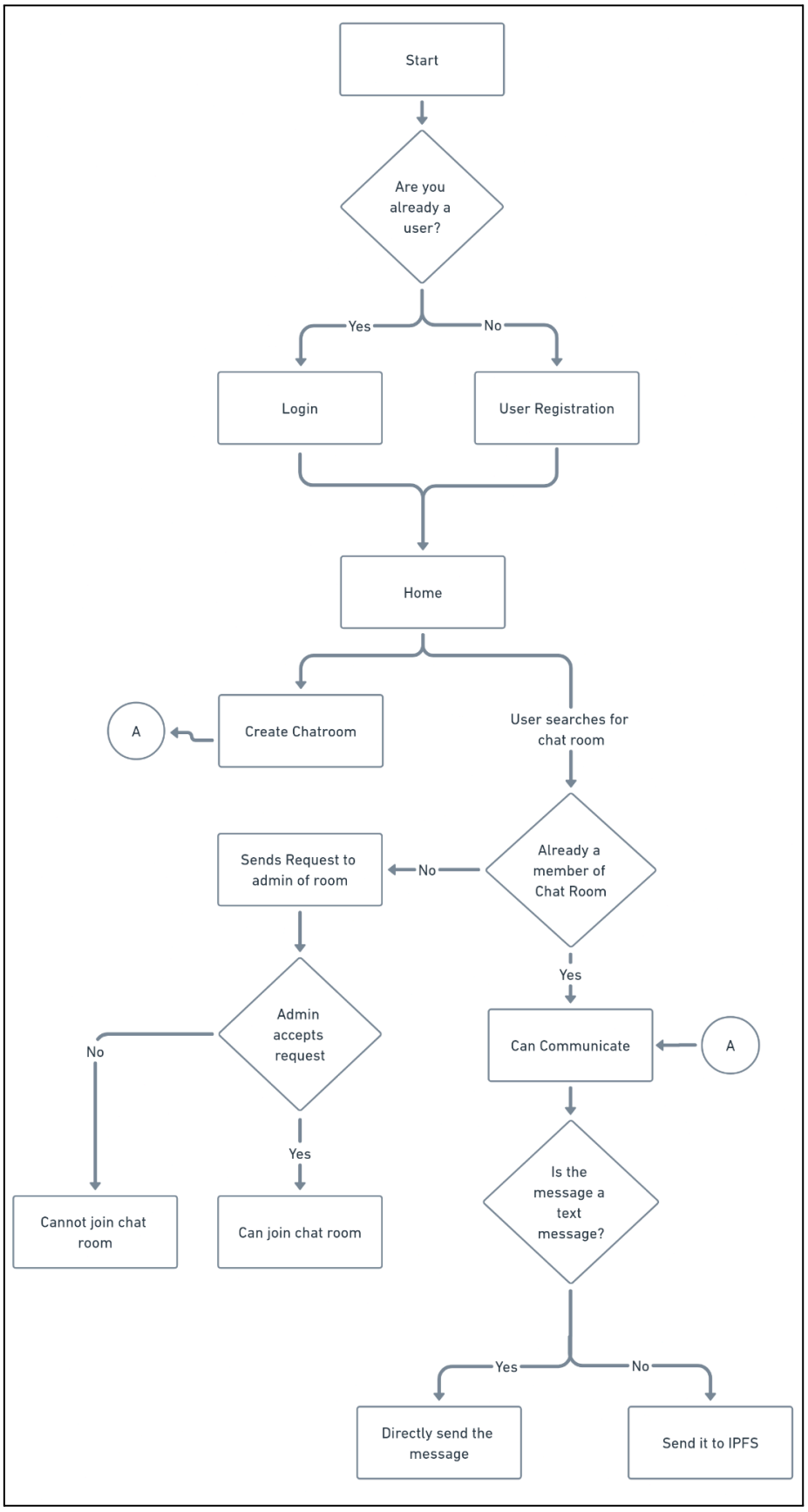

Figure 5.1: User Flow

Figure 5.1 depicts the user flow of the chat application,

- The process starts with a decision box asking the user if they are already a registered user.
- If the user is already registered, they can proceed to login and then navigate to the home screen. From there, they can search for a chatroom and request to join.
- If the user is not already registered, they will need to complete a user registration process. Once complete, they can then login and proceed to the home screen.
- Once on the home screen, users can search for existing chat rooms.
- If a user finds a chatroom they want to join, they can send a request to the admin of the room.
- The admin of the room will then decide whether or not to approve the user's request.
- If the admin approves the request, the user will be able to join the chatroom and communicate with other members.
- Once a user is a member of a chatroom, they can send messages, multimedia files, etc.
- If it is a text message, the message is directly sent to the chatroom.
- If it is not a text message, then it will need to be sent to IPFS and then sent to the other user/s.

Chapter 6: Testing of the Proposed System

6.1 . Introduction to Testing

Testing is a critical phase aimed at evaluating a system to identify defects, ensure functionality, and validate performance. It plays a pivotal role in ensuring that Aatmanirbhar Sanchar meets specified requirements and operates reliably under various conditions. The testing process encompasses functional testing to validate features, security testing to assess vulnerabilities, performance testing to evaluate responsiveness, usability testing to ensure user-friendliness, compatibility testing to verify system integration, and integration testing to validate component interactions.

6.2 Types of Tests Considered:

1. Functional Testing: Functional testing will focus on verifying the behaviour of Aatmanirbhar Sanchar against specified functional requirements. This includes testing the authentication process, message encryption and decryption, chat room creation, joining and leaving functionalities, and message exchanges within the chat rooms. The aim is to ensure that all features and functionalities work as intended, meeting user expectations for a secure communication platform.

2. Security Testing: Security testing is critical to evaluate the resilience of the chat application against potential security threats and vulnerabilities. This will involve conducting penetration testing to identify and address security weaknesses, ensuring robust encryption practices are implemented, and validating user authentication mechanisms. The objective is to fortify the application against unauthorised access, data breaches, and other security risks.

3. Performance Testing: Performance testing will assess the responsiveness and scalability of the chat application under varying load conditions. This includes measuring response times for message delivery, evaluating system stability under peak user loads, and ensuring efficient handling of media file transfers. The goal is to optimize system performance and ensure reliable operation during peak usage periods.

4. Usability Testing: Usability testing aims to gauge the user-friendliness and intuitiveness of the chat application's interface. This involves collecting user feedback on navigation, message composition, chat room management, and overall user experience. The objective is to enhance usability and address any usability issues to improve user adoption and satisfaction.

5. Compatibility Testing: Compatibility testing will verify the chat application's compatibility with different devices, operating systems, and web browsers. This includes testing across various platforms (e.g., Android, iOS, web browsers) to ensure consistent functionality and appearance. The goal is to ensure a seamless user experience across diverse environments.

6. Integration Testing: Integration testing focuses on validating the interactions between different components and modules of the chat application. This includes testing the integration of Hyperledger Fabric, IPFS, and the user interface components (e.g., ReactJS, ExpressJS). The aim is to ensure that all components work together harmoniously to deliver a cohesive and secure communication platform.

6.3 Various Test Case Scenarios Considered:

1. Mobile-to-Mobile Communication: This scenario involves testing communication between two mobile devices using the chat application. Test cases will assess message delivery, encryption, and responsiveness between mobile clients.

2. Web App to Mobile Communication: This test case scenario examines communication between a web-based client and a mobile client. It validates cross-platform compatibility, ensuring seamless message exchange and data integrity.

3. Distance Communication: This scenario evaluates communication over long distances, assessing how the application handles latency, network disruptions, and message delivery across different geographical locations.

4. Message Sending Communication: Test cases under this scenario focus on the core functionality of sending and receiving text messages. It includes verifying message delivery, display accuracy, and proper encryption.

5. File Share Communication: This scenario involves testing file-sharing capabilities within the chat application. Test cases assess the upload, download, and integrity of shared files, ensuring secure and efficient data transfer.

6.4 Inference Drawn from the Test Cases:

The test cases conducted on Aatmanirbhar Sanchar provide compelling insights into its performance and functionality across various communication scenarios. Results demonstrate the application's robustness in facilitating mobile-to-mobile communication, ensuring reliable message delivery and responsiveness on handheld devices. Additionally, tests involving web app to mobile communication showcase seamless cross-platform compatibility, underscoring the application's versatility across different interfaces. Evaluations of distance communication highlight the system's effectiveness in handling latency. Furthermore, file-sharing tests demonstrate efficient upload and download processes, reinforcing the application's ability to securely transmit files. The time taken for text communication is approximately 3 seconds, ensuring swift message delivery. Moreover, file size and time limit tests conducted between two machines located 20 kilometers apart reveal impressive performance metrics. For files up to 40 MB, transmission takes less than 30 seconds, while files up to 100 MB are transferred in less than a minute, completing under 45 seconds. Aatmanirbhar Sanchar supports various file types, including images, videos, audios, models, .deb, and more, offering comprehensive file-sharing capabilities to users.

Chapter 7: Results and Discussions

7.1. Screenshots of Chat Application User Interface (UI)

1. Registration Page :

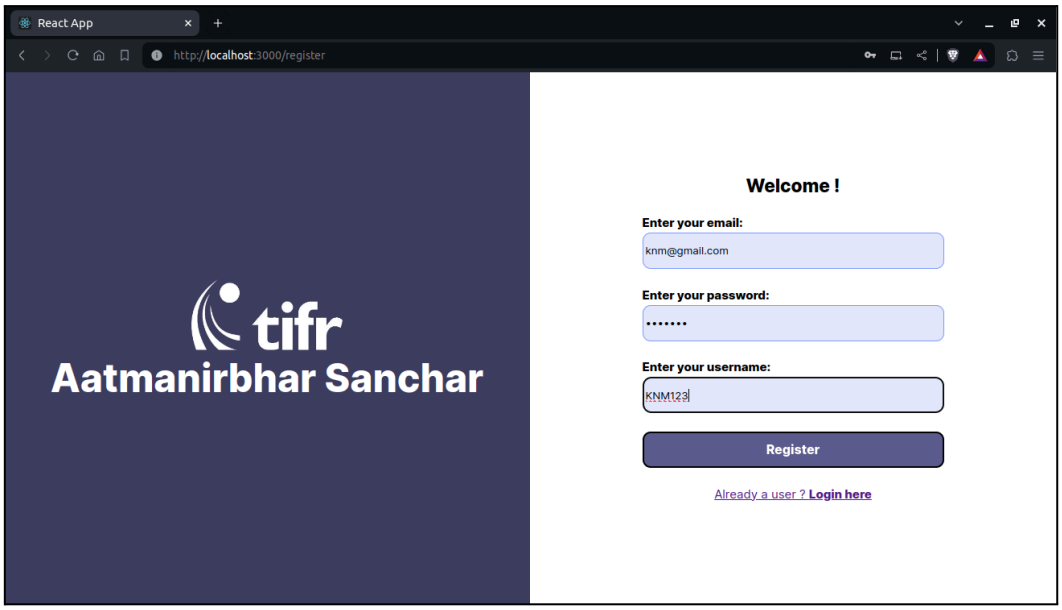

Figure 7.1: Registration Page

2. Existing Chats :

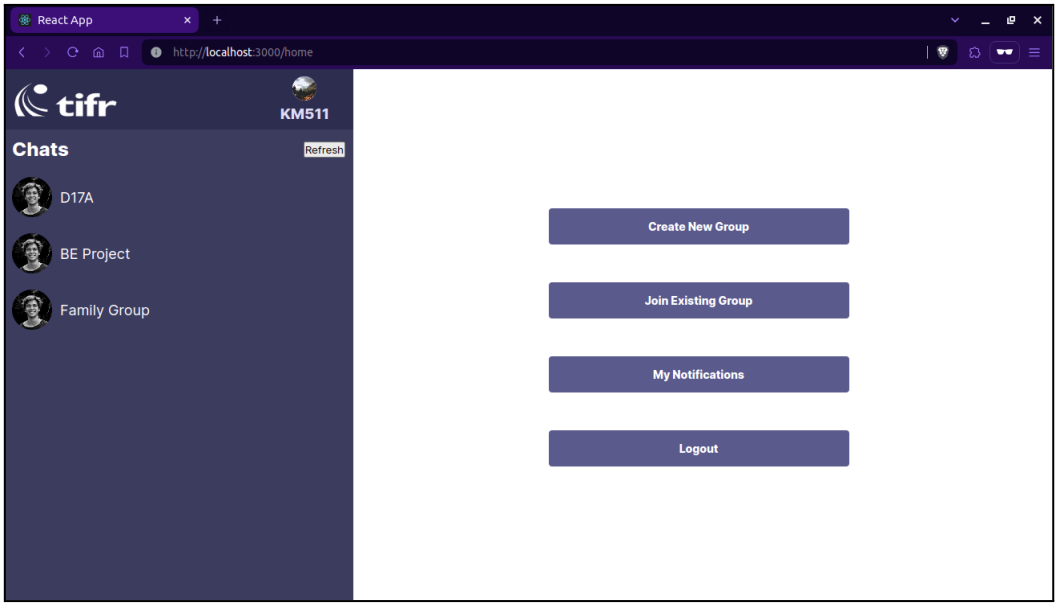

Figure 7.2: Home Page

3. Text Message Sending :

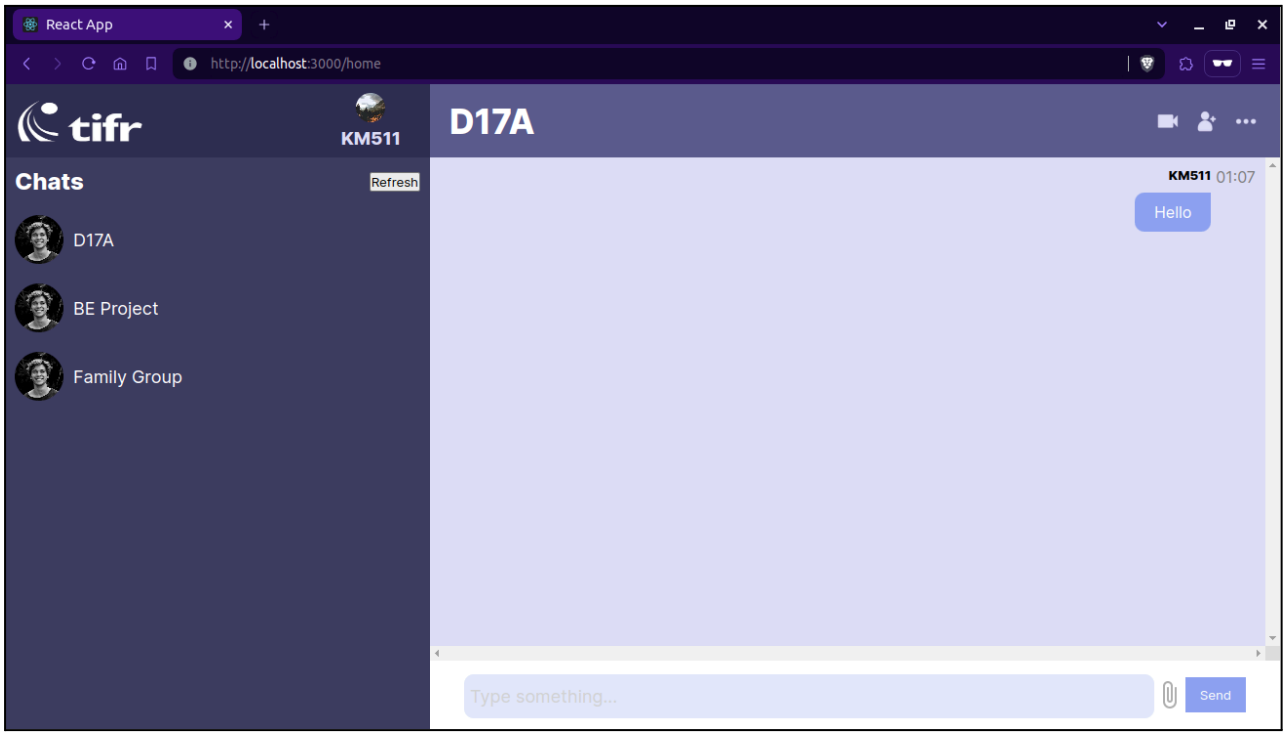

Figure 7.3: Chat Window

4. Join a New Chatroom :

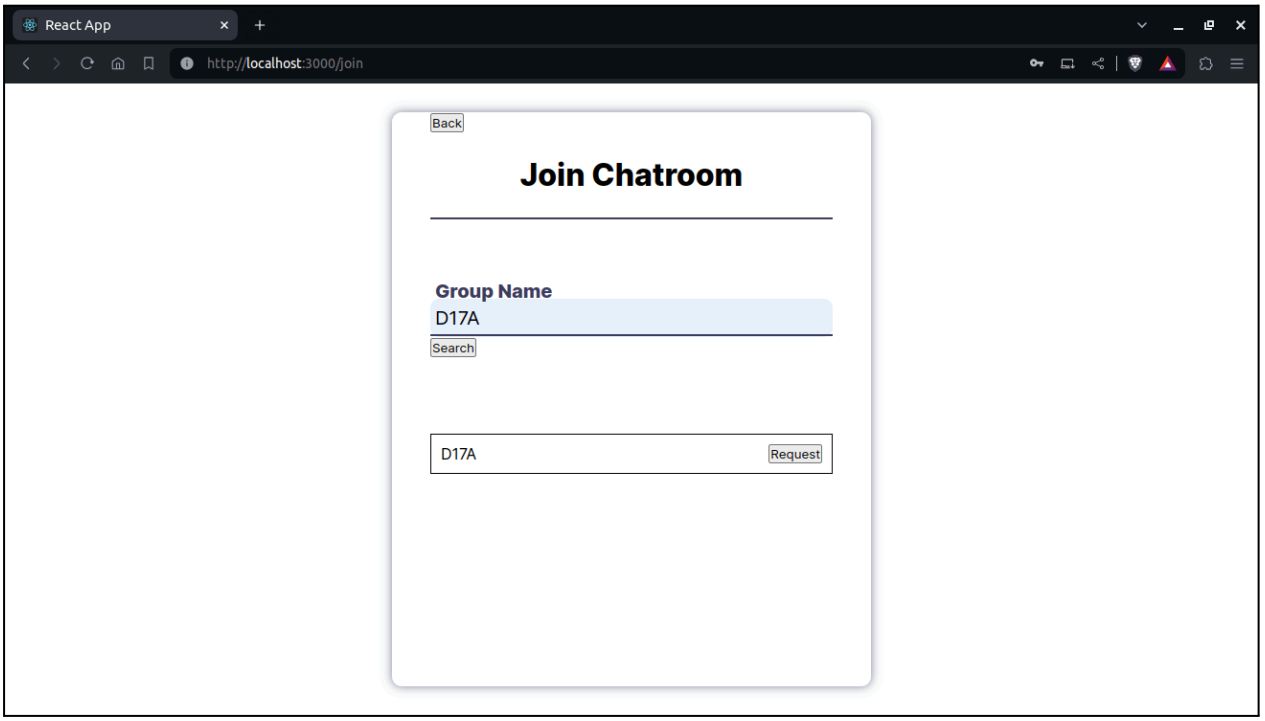

Figure 7.4: Joining new chat room feature

5. Notifications :

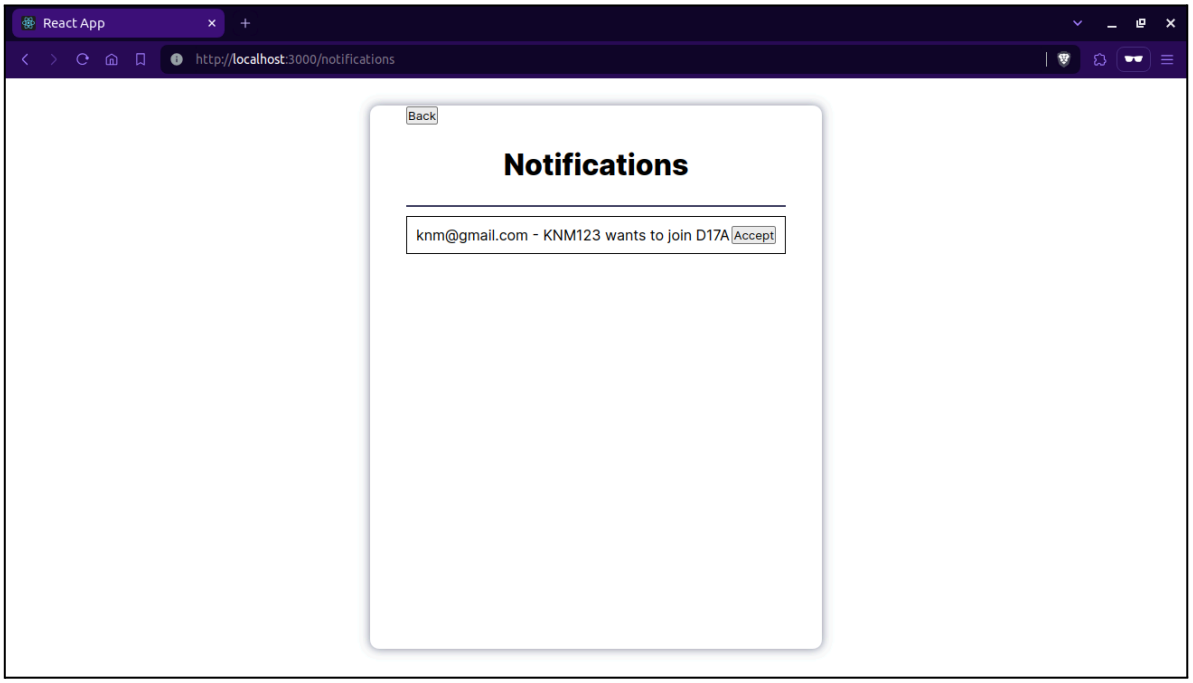

Figure 7.5: Notification window of the chat application

6. Join Chat Room Request Accepted :

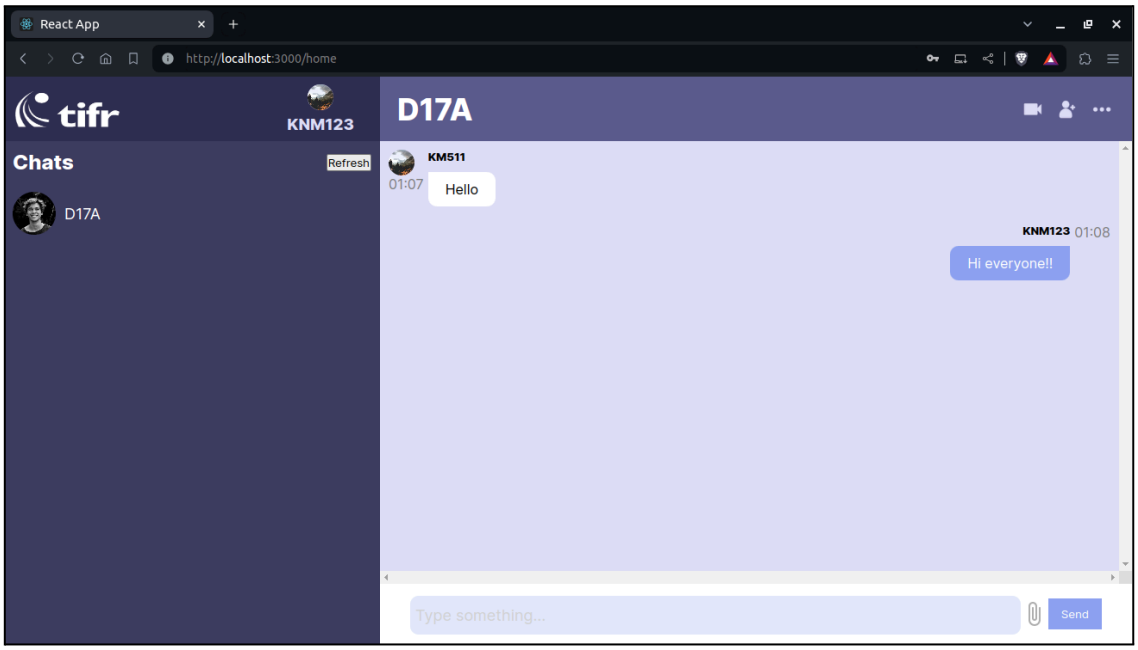

Figure 7.6 : Join Chat Room Request Accepted

7. Image/Audio/Video File Sharing :

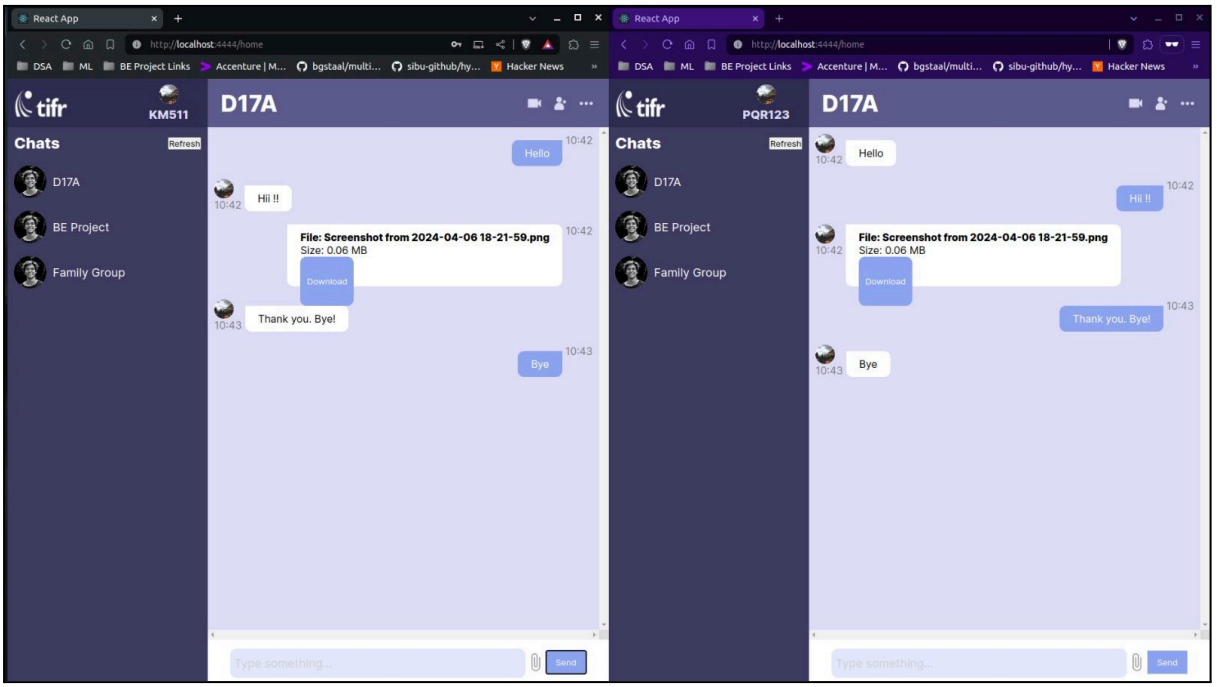

Figure 7.7: Media Sharing

8. File Download:

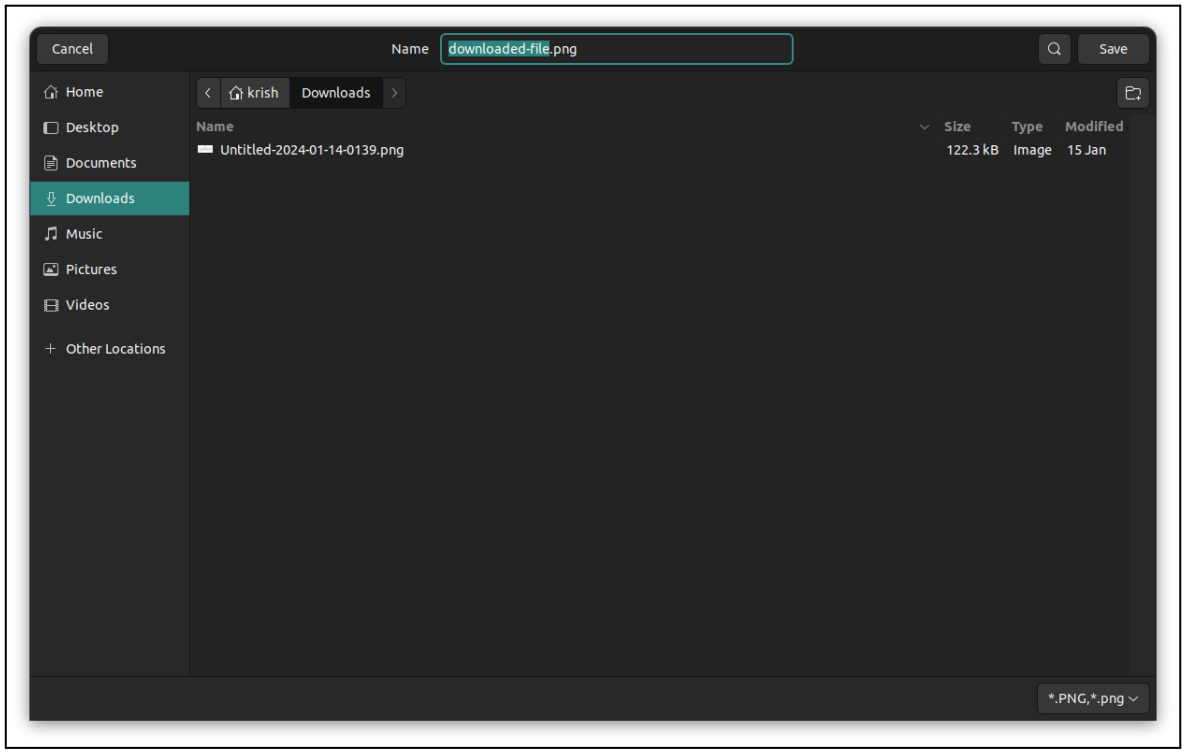

Figure 7.8: File Download

7.2. Performance Evaluation Measures:

The performance of Aatmanirbhar Sanchar will be assessed using several key metrics. These include Authentication Time (ms), Message Transmission Latency (ms), Throughput (TPS), Resource Utilization (CPU, Memory, Network Bandwidth, Storage), Data Retrieval Time from IPFS (ms), Consensus Time in Hyperledger Fabric (ms), and Security Metrics (Unauthorized Access Attempts, Detected Security Threats, Data Integrity Violations). These metrics will provide insights into the system's efficiency, scalability, security, and reliability, with lower values indicating better performance and higher security.

7.3. Input Parameters Considered:

The input parameters considered for evaluating the performance of Aatmanirbhar Sanchar include the Number of Concurrent Users, Message Size, Network Latency, Blockchain Network Size, IPFS Node Availability, Encryption Algorithm Overhead, and Blockchain Transaction Complexity. These parameters will be systematically varied and tested to assess their impact on the system's performance, scalability, and security.

7.4. Graphical and Statistical Output:

The test cases conducted on Aatmanirbhar Sanchar provide compelling insights into its performance and functionality across various communication scenarios. Results demonstrate the application's robustness in facilitating mobile-to-mobile communication, ensuring reliable message delivery and responsiveness on handheld devices. Additionally, tests involving web app to mobile communication showcase seamless cross-platform compatibility, underscoring the application's versatility across different interfaces. Evaluations of distance communication highlight the system's effectiveness in handling latency. Furthermore, file-sharing tests demonstrate efficient upload and download processes, reinforcing the application's ability to securely transmit files. The time taken for text communication is approximately 3 seconds, ensuring swift message delivery. Moreover, file size and time limit tests conducted between two machines located 20 kilometers apart reveal impressive performance metrics. For files up to 40 MB, transmission takes less than 30 seconds, while files up to 100 MB are transferred in less than a minute, completing under 45 seconds. Aatmanirbhar Sanchar supports various file types, including images, videos, audios, models, .deb, and more, offering comprehensive file-sharing capabilities to users.

Sr. No.	Type of Communication	Distance	File Size	Transmission Time
1	Mobile to mobile	100m	300kb	less than 5s
2	Mobile to mobile	100m	40mb	~ 35s
4	Desktop to mobile	20km	40mb	~ 30s
5	Desktop to mobile	20km	100mb	~ 1 min
6	Desktop to desktop	20km	40mb	~ 25s
7	Desktop to desktop	20km	100mb	~ 45s

Table 7.1 : Performance and functionality across various communication scenarios

7.5. Comparison of Results with Existing Systems:

Aatmanirbhar Sanchar aims to address several shortcomings observed in existing systems, which include limited adoption due to a preference for established platforms, scalability issues leading to slow message processing on some blockchain networks, high transaction fees acting as a barrier for frequent messaging, and challenging integration with existing systems that limits usability. By addressing these challenges, the proposed system seeks to offer a more secure, efficient, and user-friendly communication platform.

7.6. Inference Drawn:

The evaluation of Aatmanirbhar Sanchar has illuminated its exceptional features, notably its advanced security measures and unwavering commitment to user privacy. By leveraging blockchain technology, the application encrypts messages end-to-end, ensuring that user communications remain confidential and shielded from unauthorized access. The decentralized architecture of the blockchain network fortifies the platform's security, mitigating the risks associated with centralized data storage and potential breaches. Furthermore, the absence of transaction fees sets Aatmanirbhar Sanchar apart, offering users

a cost-effective solution for secure communication without any financial burden. This combination of robust security, privacy protection, and zero transaction fees establishes Aatmanirbhar Sanchar as a reliable and accessible platform for users seeking a seamless and secure communication experience.

Chapter 8: Conclusion

8.1 Limitations

Aatmanirbhar Sanchar showcases significant advancements in digital communication by leveraging cutting-edge blockchain technology, specifically Hyperledger Fabric and Interplanetary File System (IPFS). This innovative platform ensures enhanced security, privacy, and decentralized control, providing users with a trustworthy and secure environment for online communication. The transparent and tamper-proof nature of the blockchain ensures robust user authentication, secure message storage, and unparalleled transparency in communication. However, the application faces several challenges that could potentially hinder its widespread adoption and optimal performance. These include the entrenched user preference for established chat platforms, scalability issues causing slow message processing and the complexity of integrating the decentralized system with existing infrastructure. Addressing these limitations is crucial to optimize the application's performance, enhance user experience, and increase its competitiveness in the digital communication landscape.

8.2 Conclusion

Aatmanirbhar Sanchar is a new platform using blockchain technology to make online chatting more secure and private. It has strong user authentication to make sure only the right people can access the platform and chat safely. The application also uses advanced encryption to keep messages private and safe from any unauthorised access or changes. By using Hyperledger Fabric and Interplanetary File System (IPFS), the application ensures that messages are stored securely and transparently. All user actions, from logging in to sending messages, are recorded on an unchangeable blockchain ledger, making the platform trustworthy and eliminating the need for middlemen. Additionally, the application allows for anonymous communication and automatically deletes messages once the conversation ends, enhancing user privacy and security. In conclusion, Aatmanirbhar Sanchar offers a more secure and private way for people to communicate online. It addresses the shortcomings of traditional chat platforms and sets a new standard for digital communication by emphasising security, privacy, and innovation.

8.3 Future Scope

Aatmanirbhar Sanchar has established a strong foundation in the digital communication landscape through its innovative use of blockchain technology. Moving forward, there is significant potential to enhance the platform's scalability and improve the user interface and experience. Additionally, exploring integration opportunities with other platforms and expanding the range of features and functionalities can further optimize the application and broaden its appeal to a wider audience, setting the stage for continued innovation and growth in the digital communication era.

References

[1] Keshav Khalkar et al. “Decentralized ChatApplication using Blockchain Technology”, JETIR, Volume 10, Issue 5, May 2023. Available at: https://www.jetir.org/papers/JETIR2305B41.pdf

[2] I. Lokhande, N. Deotale, B. Mali, S. Chauhan and J. Dhuri, “BlockChain Based Chat Application, ” 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 2023, pp. 1-6, doi: 10.1109/INCET57972.2023.10170739. Available at: https://ieeexplore.ieee.org/document/10170739

[3] Jay Ravi Jhaveri, Prem Vinod Chabbria, Neeraj Narain Ochani, Abhay Anupam Gupta, Dr. Sharmila Sengupta, Prof. Sunita Suralkar, Prof. Shashi Dugad, “Aatmanirbhar Sanchar: Self-Sufficient Communications” . In: Hemanth, J., Pelusi, D., Chen, J.IZ. (eds) Intelligent Cyber Physical Systems and Internet of Things. ICoICI 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 3. Springer, Cham. https://doi.org/10.1007/978-3-031-18497-0_41 Available at : https://link.springer.com/chapter/10.1007/978-3-031-18497-0_41

[4] Nizamuddin, Nishara & Hasan, Haya & Salah, Khaled. (2018). “IPFS-Blockchain-Based Authenticity of Online Publications”, 10.1007/978-3-319-94478-4_14. Available at : https://www.researchgate.net/publication/325899234_IPFS-Blockchain-Based_Authenticity_of_Online_Publications

[5] Khan, Faraz & Mantri, Niraj & Rajput, Sagar & Dhakane, Dhananjay & Padiya, Puja. (2020). “Anonymous De-centralized Ephemeral Chat Application using Interplanetary File System.”, ITM Web of Conferences. 32. 02004. 10.1051/itmconf/20203202004. Available at : https://www.itm-conferences.org/articles/itmconf/pdf/2020/02/itmconf_icacc2020_02004.pdf

[6] N. Baygin, M. Baygin and M. Karakose, "Blockchain Technology: Applications, Benefits and Challenges," 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, 2019, pp. 1-5, doi: 10.1109/UBMYK48245.2019.8965565. Available at : https://ieeexplore.ieee.org/document/8965565

[7] M. S. I. Bhuiyan, A. Razzak, M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque and S. Tarkoma, "BONIK: A Blockchain Empowered Chatbot for Financial Transactions," 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 2020, pp. 1079-1088, doi: 10.1109/TrustCom50675.2020.00143. Available at : https://ieeexplore.ieee.org/document/9343092

[8] Fauziah, Noveline & Rachmawanto, Eko & Setiadi, De Rosal Ignatius Moses & Sari, Atika. (2018). “Design and Implementation of AES and SHA-256 Cryptography for Securing Multimedia File over Android Chat Application” 146-151. 10.1109/ISRITI.2018.8864485. Available at : https://www.researchgate.net/publication/336559998_Design_and_Implementation_of_AES_and_SHA-256_Cryptography_for_Securing_Multimedia_File_over_Android_Chat_Application

[9] R. Bhatangar and V. B. Lobo, "Multihop Concurrent Big Data Sharing via Multithreading using Blockchain on a Decentralized Network," 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Greater Noida, India, 2020, pp. 885-890, doi: 10.1109/ICACCCN51052.2020.9362977. Available at : https://ieeexplore.ieee.org/document/9362977

[10] M. Ahmed, S. Reno, N. Akter and F. Haque, "Securing Medical Forensic System Using Hyperledger Based Private Blockchain," 2020 23rd International Conference on Computer and Information Technology (ICCIT), DHAKA, Bangladesh, 2020, pp. 1-6, doi: 10.1109/ICCIT51783.2020.9392686. Available at : https://ieeexplore.ieee.org/document/9392686

Appendix

a. Paper in final draft and review stage

b. Project review sheet

Inhouse/ Industry _Innovation/Research:

Sustainable Goal: Industry, Innovation & Infrastructure

Project Evaluation Sheet 2023 - 24

Class: D17 A/~~B/C~~

Group No.: 48

Title of Project: Atmanirbhar Sanchar - Secure Multimedia Communication

Group Members: Hitakrit 19 Goplani, Shruti 12 Dalvi, Swara 47 Nabar, Krish 42 Mehta (D17A)

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
4	4	4	3	4	2	2	2	2	2	3	2	3	3	4	44

Comments:

~~Nusrat~~ Ansari

Name & Signature Reviewer1

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
4	4	4	3	4	2	2	2	2	2	3	3	3	3	4	45

Comments:

Date: 10th february, 2024

Name & Signature Reviewer 2

Inhouse/ Industry _Innovation/Research:

Sustainable Goal:

Project Evaluation Sheet 2023 - 24

Class: D17 A/B/C

Group No.: 48

Title of Project: Atmanirbhar Sanchar : Chat Application

Group Members: Hitakrit 19 Goplani , Shruti 12 Dalvi, Swara 47 Nabar, Krish 42 Mehta (D17A)

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
4	4	4	3	4	2	2	2	2	2	3	3	3	3	2	43

Comments: Research paper needs rework , add encrypt part as well

Nusrat Ansari

Name & Signature Reviewer1

Engineering Concepts & Knowledge (5)	Interpretation of Problem & Analysis (5)	Design / Prototype (5)	Interpretation of Data & Dataset (3)	Modern Tool Usage (5)	Societal Benefit, Safety Consideration (2)	Environment Friendly (2)	Ethics (2)	Team work (2)	Presentation Skills (2)	Applied Engg&Mgmt principles (3)	Life - long learning (3)	Professional Skills (3)	Innovative Approach (3)	Research Paper (5)	Total Marks (50)
4	4	4	3	4	2	2	2	2	2	3	3	3	3	2	43

Comments: Research Paper

Date: 9th March, 2024

Name & Signature Reviewer 2