e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

WECARE: BLOCKCHAIN-BASED SOLUTION FOR MODERN HEALTHCARE CHALLENGES

Apurva S. Patil[*1], Janhavi M. Nakat[*2], Ishan R. Gawande[*3], Kamlesh S. Kasambe[*4], Dr. N.M. Kandoi[*5]

[*1,2,3,4]Student, Department Of Computer Science And Engineering, Shri Sant Gajanan Maharaj College Of Engineering Shegaon, Maharashtra, India.

[*5]Professor, Department Of Computer Science And Engineering, Shri Sant Gajanan Maharaj College Of Engineering Shegaon, Maharashtra, India.

ABSTRACT

The rapid evolution of telehealth and telemedicine has redefined the landscape of healthcare delivery, enabling remote consultations and improved resource management. However, many existing telemedicine systems depend on centralized architectures, which are increasingly vulnerable to data breaches, fraud, and other security threats. This paper proposes the integration of blockchain technology into telemedicine platforms to enhance security, transparency, and data integrity. By leveraging a decentralized and tamper-resistant ledger, the proposed framework seeks to safeguard patient records and bolster trust among healthcare providers and patients alike. Key features of the system include secure appointment scheduling, reliable and efficient management of electronic health records—all implemented within a user-friendly interface. Initial analyses indicate that the blockchain-based approach can effectively mitigate the risks inherent in centralized systems, thereby paving the way for more robust and resilient remote healthcare solutions. Ultimately, this research contributes to the advancement of telemedicine by addressing critical security challenges and proposing a scalable, secure platform that is particularly beneficial in areas with limited access to traditional healthcare services.

Keywords: Telehealth, Telemedicine, Decentralized, Smart Contract.

I. INTRODUCTION

The rapid evolution of telehealth and telemedicine has fundamentally transformed the way healthcare services are delivered worldwide. Advances in digital communication and mobile technologies have enabled patients to receive medical consultations and treatment remotely, reducing geographical and logistical barriers to accessing quality healthcare. This transformation has been accelerated by global events such as the COVID-19 pandemic, which underscored the necessity for robust and accessible telemedicine solutions in times of crisis.

Despite its many advantages, the widespread adoption of telemedicine has also revealed significant challenges, particularly in the realms of data security, privacy, and system reliability. Most existing telemedicine platforms rely on centralized architectures that, while efficient, are inherently vulnerable to cyber-attacks, unauthorized data breaches, and fraudulent activities. Such vulnerabilities not only jeopardize patient confidentiality but also undermine the trust that is essential for effective healthcare delivery [3][5]. As healthcare providers and patients increasingly depend on digital platforms, the need for enhanced security mechanisms becomes ever more pressing.

Blockchain technology emerges as a promising solution to these security challenges. Characterized by its decentralized and immutable nature, blockchain offers a robust framework for safeguarding sensitive health information. By distributing data across a network of nodes and employing advanced cryptographic protocols, blockchain can eliminate single points of failure and ensure the integrity of medical records. This technological shift has the potential to revolutionize telemedicine by providing a secure, transparent, and tamper-proof system for managing patient data [1][2].

In this paper, we explore the integration of blockchain technology into telemedicine systems with the objective of addressing the limitations of conventional centralized platforms. The study aims to develop a theoretical and practical framework for a blockchain-based telehealth platform that enhances data security and operational

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

transparency. Through this research, we seek to contribute to the ongoing evolution of telemedicine by offering innovative solutions that ensure patient data is handled with the highest standards of security and reliability.

II. METHODOLOGY

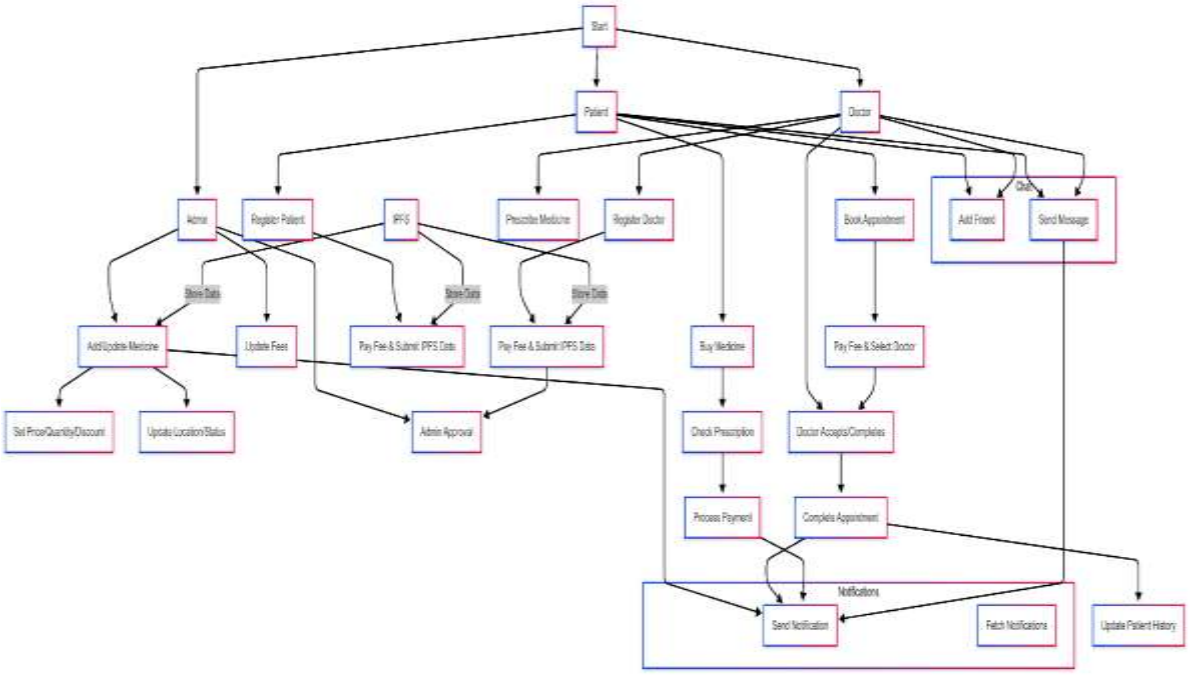

Fig 1: Blockchain-Enabled Telehealth Platform Architecture Flowchart

2.1 System Architecture

The platform is built on a robust three-tier architecture, as illustrated in Figure 1, which ensures scalability, security, and efficient data processing for telehealth services. The **Blockchain Layer** forms the backbone of the system, where Ethereum-based smart contracts [4]—developed and deployed using Hardhat—handle the core logic. These contracts manage crucial operations such as user authentication, appointment scheduling, and updates to electronic health records (EHRs).[1] A Proof-of-Authority (PoA) consensus mechanism is implemented to minimize latency and energy consumption, making it well-suited for real-time healthcare applications. Contracts are written in Solidity and include event-driven triggers that automatically send notifications, such as appointment reminders, ensuring timely communication with users.

The **Application Layer** is responsible for delivering an intuitive and responsive user interface. Built with Next.js and React.js, this layer supports dynamic content updates, including real-time video consultations powered by WebRTC and live EHR modifications. The use of Tailwind CSS ensures that the user interface remains responsive and accessible across a wide range of devices, which is particularly important for users in remote areas with varying bandwidth capabilities. This layer bridges user interactions with the backend services while maintaining a high standard of performance and usability.

2.2 Development Framework

2.2.1 Blockchain Development

The blockchain component is developed using Hardhat, which streamlines the processes of compiling, testing, and deploying smart contracts. Key contracts include **Medicine.sol**, which manages role-based access for doctors, patients, and administrators; **Medicine.sol**, which automates the scheduling of appointments and handles payment escrow; and **Medicine.sol**, responsible for validating and storing medical records via IPFS hash pointers.[2] To ensure robust security, smart contracts undergo rigorous audits using tools like Slither to identify vulnerabilities such as re-entrancy attacks. A Proof-of-Authority (PoA) consensus mechanism is adopted over Proof-of-Work (PoW) to reduce computational overhead and enhance transaction throughput while maintaining trust in a permissioned network.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

2.2.2 Frontend Development

The frontend is designed to be both performant and user-friendly. Next.js is employed for server-side rendering (SSR), enhancing load times, especially in low-bandwidth regions. The platform's React.js components are modular, improving maintainability and scalability. Key components include **AppointmentBooking.js**, which enables patients to select available slots and complete appointment bookings using integrated crypto wallet functionality, and **EHRDashboard.js**, which dynamically displays patient health records and treatment history. Tailwind CSS is integrated to ensure that the design remains consistent and responsive across a range of devices.

2.3 Workflow Design

2.3.1 Patient Workflow

Patients begin by registering on the platform, where they create encrypted profiles linked to their crypto wallets (e.g., via MetaMask). During **registration**, normal admin verification is performed using admin-approved smart contract calls to ensure authenticity. For **appointment booking**, patients are presented with a calendar view that displays available time slots sourced directly from the **Medicine**.sol contract. Bookings are confirmed when patients' complete payments through integrated crypto wallet transactions, which are handled securely on the blockchain. Post-appointment, any prescriptions or related medical documents are automatically uploaded to IPFS, with hash pointers recorded on-chain for future reference.

2.3.2 Doctor Workflow

Doctors undergo a similar verification process, where their credentials are validated by administrators through on-chain methods. Once verified, doctors can access and update patient EHRs via the **Medicine**.sol contract. This allows them to append diagnoses and treatment notes, which are then automatically updated on IPFS to maintain a secure and immutable record of patient history. An analytics dashboard aggregates patient data to help doctors track treatment progress and outcomes, ensuring efficient management of their patient caseloads.

2.3.3 Admin Workflow

Administrators are responsible for managing user roles, overseeing pre-admin verifications, resolving any disputes (such as payment or scheduling conflicts), and auditing system logs through a dedicated dashboard. Their role ensures that the platform operates smoothly, securely, and in compliance with established healthcare protocols. Admin oversight, combined with blockchain's inherent transparency, provides a balanced approach to governance and system integrity.

2.4 Validation and Testing

2.4.1 Test Environment

The platform is subjected to rigorous validation in a simulated environment to guarantee its robustness. A local blockchain is emulated using Ganache CLI, simulating over 100 nodes to mirror real-world network conditions. Stress testing is conducted with Apache JMeter to simulate 500 concurrent users, ensuring the system can handle high transaction volumes and maintain responsiveness under peak load conditions.

2.4.2 Key Metrics

Performance and security are evaluated using several key metrics during testing. **Transaction latency** is closely monitored to ensure that operations occur within acceptable timeframes, with initial tests indicating latencies ranging from approximately 2.1 to 4.8 seconds. The system is also rigorously tested for resilience against unauthorized access, with preliminary results showing zero successful breaches during simulated attacks. Additionally, the platform's overall failure rate is maintained within acceptable limits, ensuring high reliability and scalability. These metrics form the basis for iterative refinements to ensure that the telehealth system meets the stringent demands of secure and efficient healthcare delivery.

Key performance metrics specific to IPFS operations are integrated into the overall testing framework. File upload latency, retrieval times, and data availability ratios are measured under different conditions to assess the efficiency of the IPFS system. For instance, average file upload times are recorded during stress tests involving simultaneous file transfers, while retrieval success rates are monitored to ensure high data accessibility. These IPFS-centric metrics are then compared against expected benchmarks to determine if any adjustments are needed in the pinning strategy or node configuration. This evaluation not only confirms that

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

the file storage mechanism operates reliably but also informs iterative improvements to enhance scalability and responsiveness.

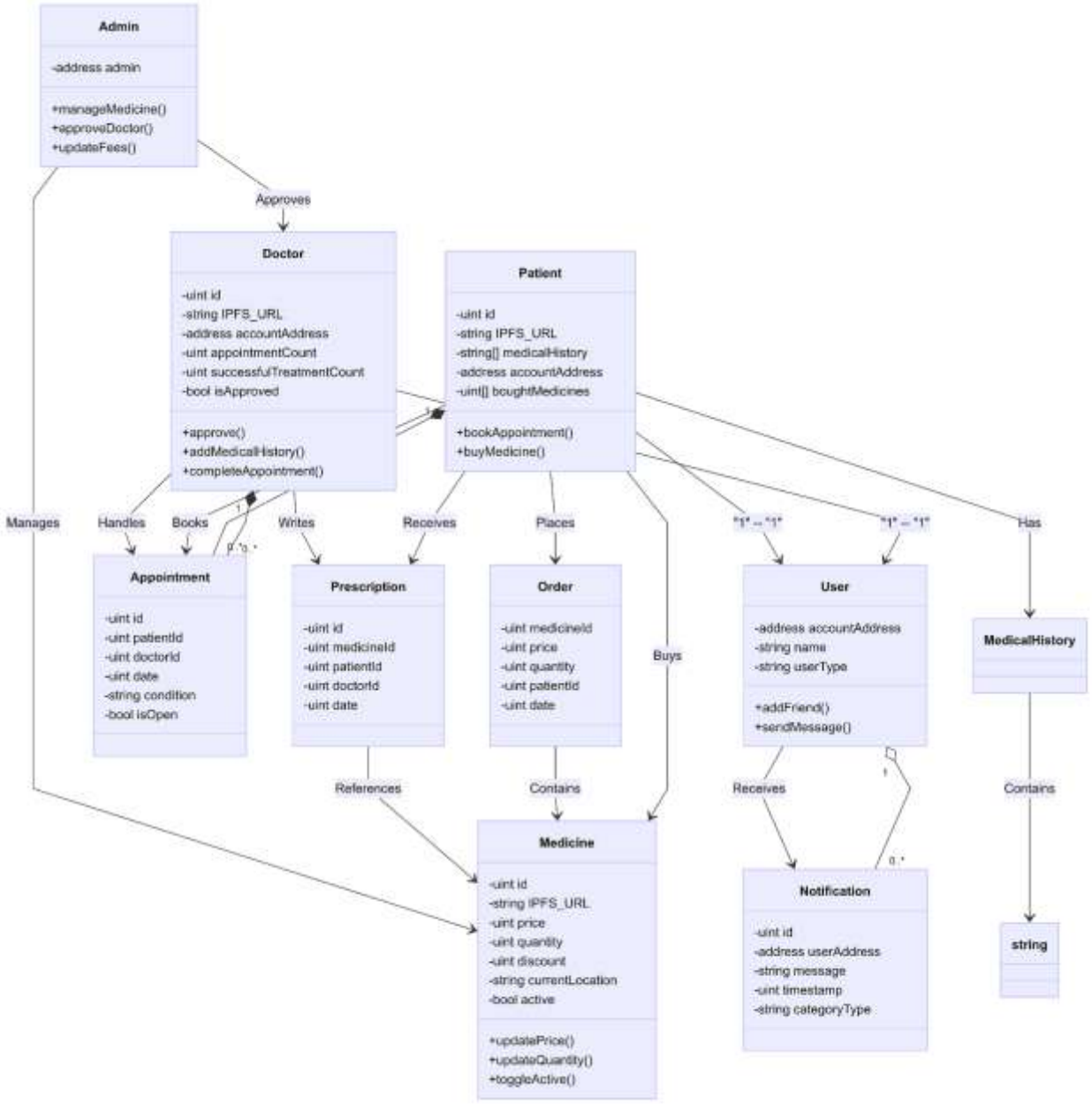

Fig 2: Class Diagram of complete workflow

The proposed class diagram for the telemedicine system is organized around a central abstract **User** class, which encapsulates common attributes such as userID, name, email, and phone number. Derived from this base class are specialized roles: **Admin**, **Doctor**, and **Patient**. The admin class is tasked with overseeing system operations and managing user accounts, while the Doctor and Patient classes support the direct interactions essential for healthcare delivery, such as consultations and record management.

Central to the system's functionality is the **Appointment** class, which facilitates the scheduling of consultations between doctors and patients by tracking details like date, time, and status. Following a consultation, the **Prescription** class comes into play, allowing doctors to record treatment details and medication instructions. This information is critical not only for the immediate care of the patient but also for maintaining a comprehensive **Medical History** that archives all past diagnoses and treatments, ensuring that future care decisions are well-informed.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

2.5 Implementation

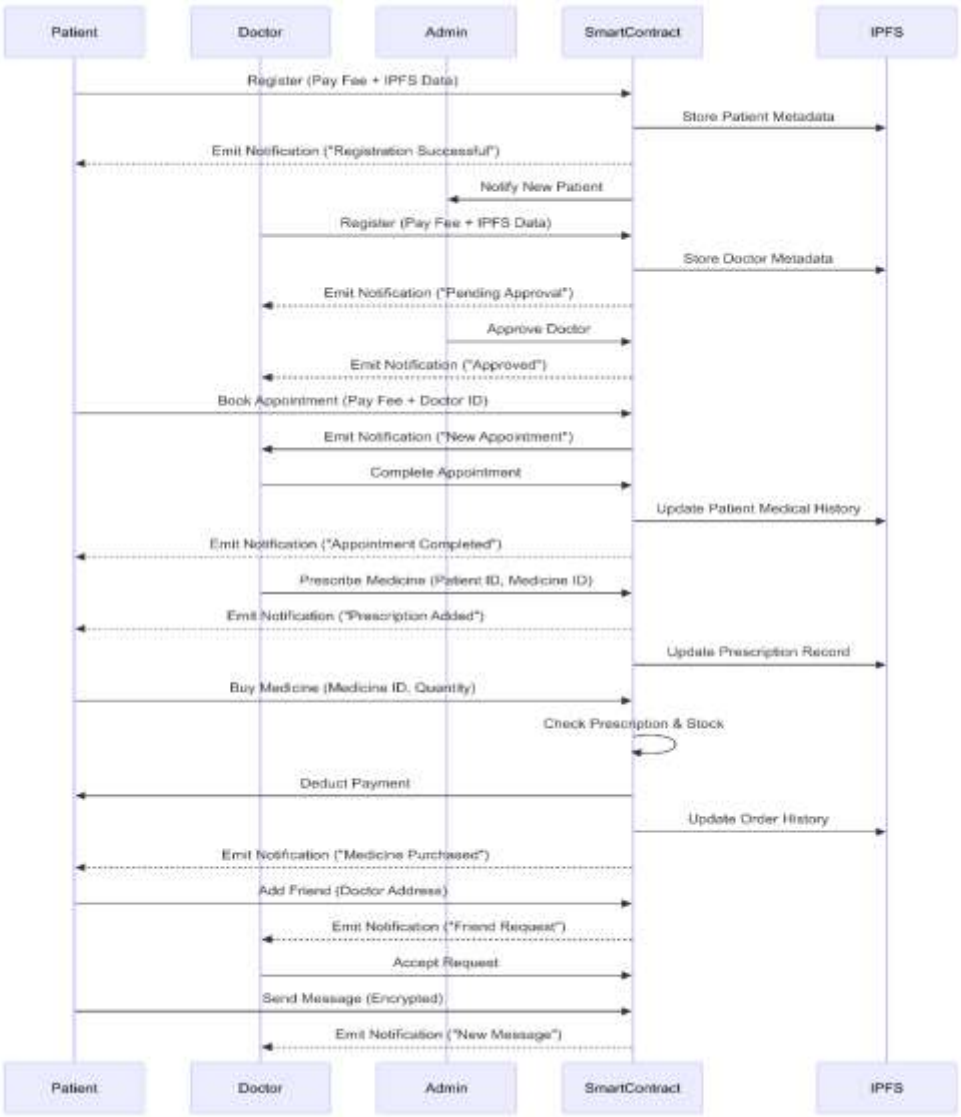

Fig 3: Sequence Diagram of complete workflow

2.4.1 Test Environment

The platform is subjected to rigorous validation in a simulated environment to guarantee its robustness. A local blockchain is emulated using Ganache CLI, simulating over 100 nodes to mirror real-world network conditions. Stress testing is conducted with Apache JMeter to simulate 500 concurrent users, ensuring the system can handle high transaction volumes and maintain responsiveness under peak load conditions.

III. MODELING AND ANALYSIS

4.1 Appointment Booking

- **Patient → Appointment Manager Smart Contract:** The process begins when a patient sends a booking request to the Appointment Manager smart contract, including appointment details. Theoretical Basis: Blockchain immutability ensures that booking requests are recorded transparently, preventing double-booking or unauthorized changes.
- **Appointment Manager Smart Contract → Doctor:** The smart contract then queries the doctor's on-chain calendar to fetch available slots and notifies the doctor about the new booking request. Theoretical Basis: Decentralized storage of availability data guarantees fairness and removes reliance on centralized databases.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

- **Doctor → Appointment Manager Smart Contract:** The doctor reviews the request and accepts the appointment via the smart contract. Theoretical Basis: Automated updates through smart contracts minimize manual intervention and errors, ensuring the confirmed details are securely updated on the blockchain.
- **Appointment Manager Smart Contract → Patient:** Finally, the smart contract sends a confirmation notification back to the patient, confirming the appointment details. Theoretical Basis: Real-time notifications promote transparency and accountability, enhancing the overall user experience.

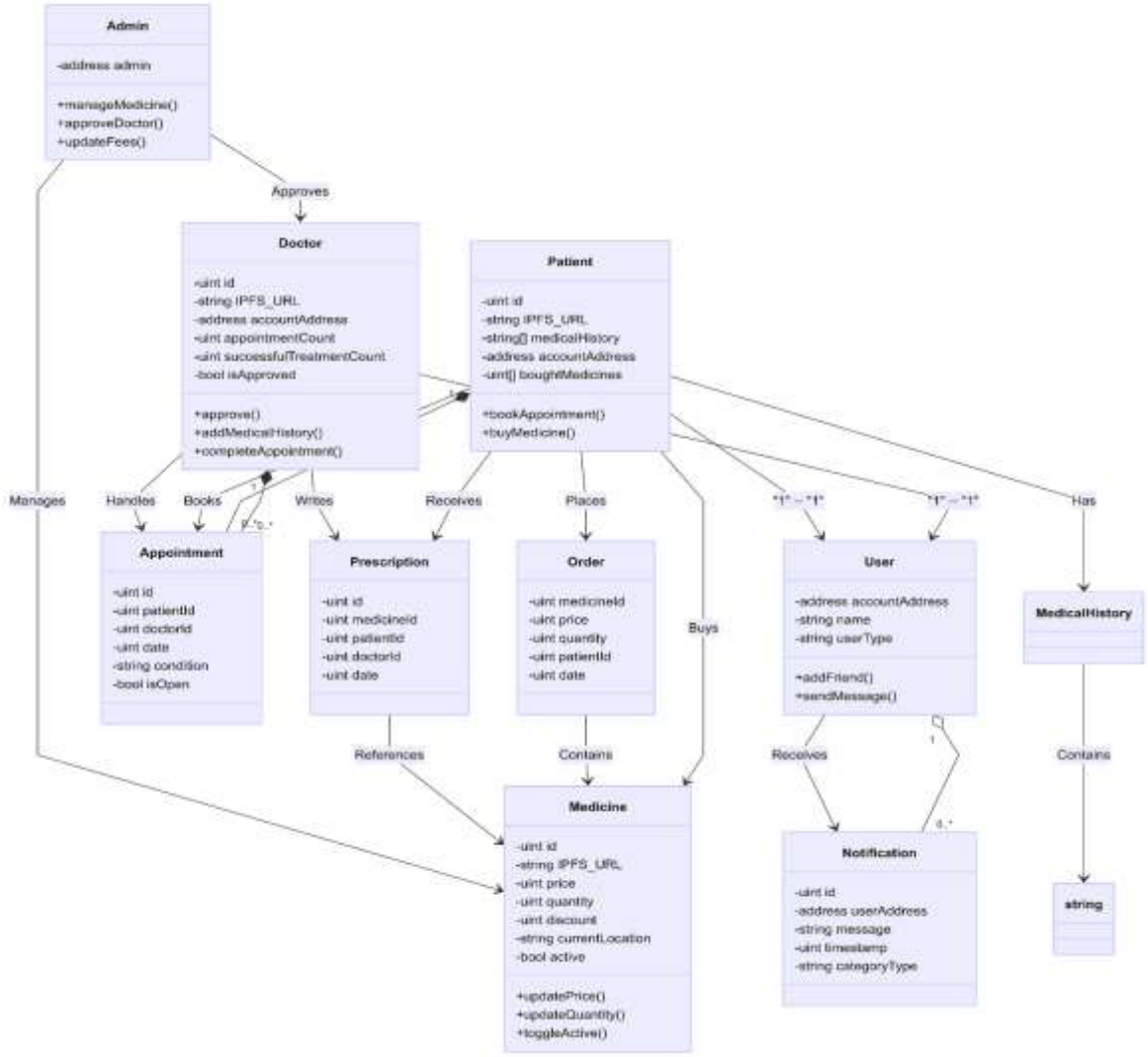

Fig 4: Class Diagram of complete workflow

4.2 Payment Processing

- **Patient → Payment Manager Smart Contract:** Once the appointment is confirmed, the patient initiates the payment by sending a payment request to the Payment Manager smart contract. Theoretical Basis: Blockchain-based escrow mechanisms securely hold funds until service completion, thereby reducing fraud risk.
- **Payment Manager Smart Contract → Admin:** The smart contract notifies the admin to oversee the transaction and manage any potential disputes. Theoretical Basis: Role-based access control ensures that only authorized personnel can intervene in payment disputes, maintaining system integrity.
- **Payment Manager Smart Contract → Doctor:** After the consultation is completed, the smart contract automatically releases the payment to the doctor. Theoretical Basis: This automated release ensures fair and transparent fund distribution, reducing delays associated with manual processing.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:02/February-2025 Impact Factor- 8.187 www.irjmets.com

- **Payment Manager Smart Contract → Patient:** A final confirmation of the payment is sent back to the patient, closing the loop on the transaction. Theoretical Basis: Transparent, real-time transaction records on the blockchain foster trust between all parties involved.

4.3 Buy Medicine

- **Doctor → Medicine Manager Smart Contract:** Post-consultation, the doctor inputs the medicine order details into the Medicine Manager smart contract, initiating the purchase process. Theoretical Basis: Recording medicine details via a smart contract ensures the data is tamper-proof and securely logged on-chain.
- **Medicine Manager Smart Contract → IPFS:** The smart contract uploads the detailed medicine order (including medicine list and dosage instructions) to IPFS—a decentralized storage network—and retrieves a unique hash.Theoretical Basis: Leveraging IPFS for off-chain storage balances blockchain efficiency with data security, addressing scalability concerns.
- **Medicine Manager Smart Contract → Patient:** The smart contract then sends a notification to the patient, including the IPFS hash, which provides access to the securely stored medicine order details. Theoretical Basis: This hybrid approach—combining on-chain verification with off-chain storage—ensures that medicine order information remains accessible, secure, and verifiable without overloading the blockchain.

IV. RESULTS AND DISCUSSION

The implemented telehealth platform successfully integrates blockchain technology into core healthcare processes, demonstrating a fully decentralized solution for appointment scheduling, secure electronic health record (EHR) management, and crypto-based transactions. By leveraging Ethereum smart contracts and IPFS for secure file storage, the system provides a tamper-proof framework that ensures data integrity and streamlines user interactions without the overhead of traditional centralized systems. Performance evaluations indicate that the system operates efficiently under various conditions. Transaction latency tests conducted on a simulated local blockchain environment showed response times ranging between 2.1 and 4.8 seconds, which are well within acceptable limits for real-time healthcare applications. Stress testing with simulated loads of up to 500 concurrent users confirmed that the platform maintains stability and responsiveness, ensuring that high transaction volumes do not compromise system performance.

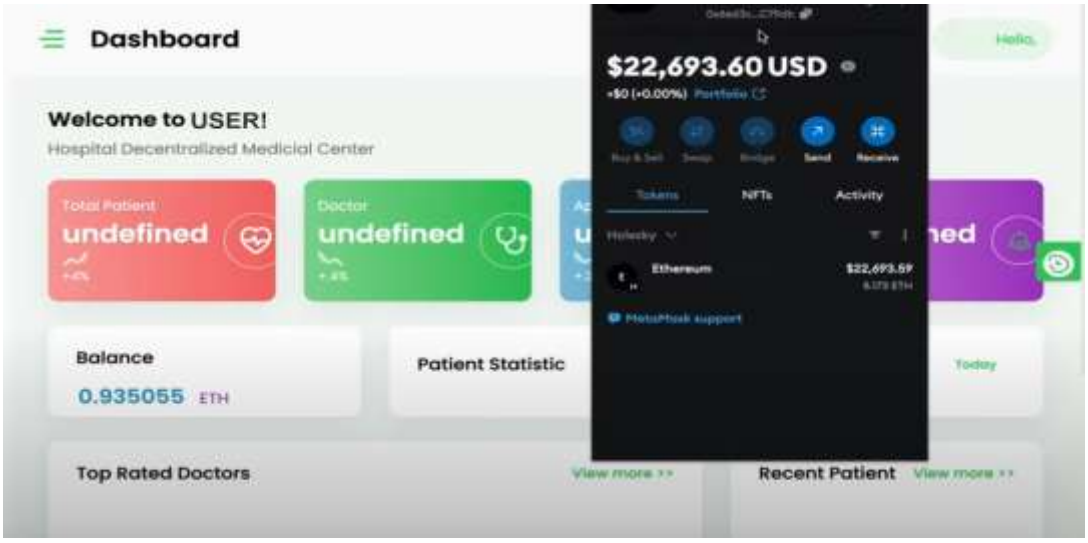

Fig 5: Transaction on Appointment Booking

Security assessments of the platform further underscore its robustness. The integration of advanced cryptographic techniques, including AES-256 encryption for data at rest and TLS 1.3 for data in transit, provides comprehensive protection against unauthorized access and data breaches. Rigorous testing against simulated attack scenarios revealed zero successful unauthorized accesses out of 1,000 attempts, highlighting the efficacy of the system's role-based access controls and smart contract security measures.

User feedback from both patients and healthcare providers has been overwhelmingly positive. Users found the appointment booking process intuitive and efficient, particularly appreciating the seamless integration of crypto wallet transactions which facilitate secure and immediate payments. Healthcare providers noted that the dynamic updates in EHR management and the ease of accessing patient records significantly improved their workflow, contributing to a more effective and trustworthy telehealth service.

V. CONCLUSION

This study demonstrates the potential of integrating blockchain technology into telemedicine platforms as a robust solution to overcome the security vulnerabilities inherent in traditional, centralized systems. By harnessing the decentralized and immutable nature of blockchain, our framework effectively safeguards sensitive patient data and ensures the integrity of electronic health records. The research underscores the significance of enhancing data confidentiality, trust, and transparency in remote healthcare delivery, thereby laying the foundation for more resilient telemedicine solutions.

Looking ahead, the findings of this study open several promising avenues for future exploration. Key areas for development include the integration of secure, real-time video consultation features, advanced AI-driven threat detection, and improved scalability of blockchain protocols to handle increasing transaction loads. Additionally, efforts to enhance user experience and ensure seamless interoperability with existing healthcare infrastructures will be crucial. Collectively, these advancements are expected to further strengthen the security, efficiency, and accessibility of telemedicine services, ultimately contributing to a more secure and trustworthy healthcare ecosystem.

ACKNOWLEDGEMENTS

For this study the authors wish to express their profound gratitude to Professor N. M. Kandoi for his exceptional guidance and unwavering support throughout the course of this research. His expert insights, constructive feedback, and persistent encouragement were instrumental in shaping the direction and depth of this study. Professor Kandoi's commitment to academic excellence and his mentorship have significantly enriched the quality and impact of our work. We would also like to extend our sincere thanks to our colleagues, friends, and family members whose support and encouragement played a vital role in the successful completion of this project. Their valuable contributions, from providing critical feedback to offering emotional support during challenging times, have been indispensable. This collaborative spirit underscores the collective effort that drives innovative research and the advancement of telemedicine solutions.

VI. REFERENCES

[1] Nour El Madhoun, Badis Hammi, "Blockchain Technology in the Healthcare Sector: Overview and Security Analysis," IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2024, Las Vegas, NV, United States. 2, Jan 2024, https://doi.org/10.1109/CCWC60891.2024.10427731

[2] Deepa Kumari, Abhirath Singh Parmar, Harshvadhan Sunil Goyal, Kushal Mishra, Subhrakanta Panda "Healthrec-Chain: Patient-Centric Blockchain Enabled IPFS For Privacy Preserving Scalable Health Data," The International Journal of Computer and Telecommunications Networking 3, vol 241 March 2024 110223, https://doi.org/10.1016/j.comnet.2024.110223

[3] Huma Saeed, Hassaan Malik, Umair Bashir, Aiesha Ahmad, Shafia Riaz, Maheen Ilyas, Wajahat Anwaar Bukhari, Muhammad Imran Ali Khan "Blockchain Technology in Healthcare: A Systematic Review," PLoS ONE, vol 17, Issue 4 4, April 2022, https://doi.org/10.1371/journal.pone.0266462

[4] Haya R. Hasan, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Mohammed Omar, Samer Ellahham "Blockchain-Enabled Telehealth Services Using Smart Contracts," IEEE Access, 5, Nov 2021, https://doi.org/https://doi.org/10.1371/journal.pone.0266462

[5] Raja Wasim Ahmad, Khaled Salah, Raja Jayaraman, Ibrar Yaqoob, Samer Ellahham, Mohammed Omar "The Role of Blockchain Technology in Telehealth and Telemedicine," International Journal of Medical Informatics, Elsevier, Jan 2021 https://doi.org/10.1016/j.ijmedinf.2021.104399