MedRec: Blockchain-Based Medico-Legal Record Handling using SHA-256 Hashing

HARSHAVARDHINI K (2127210502018)
KANIMOZHI J (2127210502020)
SRINITESH S (2127210502051)

AD18811 – PROJECT WORK

Third Review

Batch No : AD08
Name of the Internal Guide : Ms. S Janani / Assistant Professor / CSE
Date of Review : 08/05/2025
Domain : Med Tech / Bio Tech / Health Tech

SVCE

ABSTRACT

- This project develops a Flutter-based medico-legal record management system to securely store, access, and manage sensitive medico-legal documents.
- The system includes User, Hospital, and Legal Authority modules, enabling document requests, verification, and retrieval while ensuring secure data handling.
- It eliminates manual inefficiencies, unauthorized data access, record tampering, and retrieval delays by providing a structured and secure document management solution.
- It implements SHA-256 cryptographic hashing for document encryption, blockchain technology for immutable storage, and Firebase real-time database for fast and synchronized data access.
- The system enhances security, transparency, efficiency, and regulatory compliance, while reducing manual effort, preventing data loss, and ensuring role-based access to medico-legal records.
- It provides a tamper-proof, decentralized, and automated medico-legal record management system, improving data security, accessibility, and trust between hospitals, legal authorities, and users.

PROBLEM STATEMENT

- Traditional medico-legal record management relies on manual documentation, leading to inefficiencies, delays, and increased manpower requirements.
- Existing systems lack secure storage mechanisms, making records vulnerable to tampering, unauthorized access, and data breaches.
- The absence of a decentralized and immutable system results in data inconsistencies, errors, and legal disputes.
- Retrieving historical medico-legal records is time-consuming due to fragmented and unstructured databases.
- Lack of real-time synchronization between hospitals and legal authorities leads to delays in case investigations and document verification.
- There is a need for an integrated, blockchain-powered system with SHA-256 encryption to ensure secure, tamper-proof, and efficient medico-legal record management.

INTRODUCTION

- MedRec is a Flutter-based medico-legal record management system designed to ensure secure, efficient, and tamper-proof storage of medico-legal records.
- The system integrates SHA-256 cryptographic hash function to encrypt and protect sensitive documents from unauthorized access and data breaches.
- Blockchain technology ensures immutable record storage, enhancing transparency and preventing data manipulation.
- Firebase real-time database enables fast and seamless access to medico-legal records for users, hospitals, and legal authorities.
- Role-based access control (RBAC) ensures that hospitals can securely upload medical and legal records, legal authorities can retrieve case-related documents, and users can access certified records.
- MedRec enhances security, traceability, and compliance, reducing search time and manpower while ensuring efficient medico-legal record management.

LITERATURE REVIEW (1/8)

Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning, Journal of Network and Computer Applications, Volume 224, 2024.

- This study presents an optimized blockchain-based healthcare framework, IP-HealthChain, which integrates blockchain with mixed multi-agent reinforcement learning (MARL) to enhance security, decentralization, and efficient data exchange in healthcare systems.
- The paper proposes a blockchain-based optimization model using a Mixed Decentralized Partially Observable Markov Decision Process (MD-POMDP). It employs deep reinforcement learning techniques, specifically Deep Multi-Agent Q-Learning, to optimize decision-making, improve resource allocation, and enhance system security while reducing latency and costs.
- The study identifies key challenges, including the complexity of integrating blockchain with healthcare systems, high computational requirements for MARL-based optimization, and the need for real-time scalability. Additionally, regulatory and ethical concerns regarding data privacy and security remain major hurdles.

LITERATURE REVIEW (2/8)

Alessandra Rizzardi, Sabrina Sicari, Jesus F. Cevallos M., Alberto Coen-Porisini, IoT-driven blockchain to manage the healthcare supply chain and protect medical records, Future Generation Computer Systems, Volume 161, 2024.

- The study presents an IoT-driven blockchain framework to enhance security, traceability, and efficiency in managing the healthcare supply chain and protecting medical records.
- The proposed system integrates IoT with Hyperledger Fabric, a permissioned blockchain, to ensure secure data exchange and enforce access control policies via smart contracts. Performance evaluation was conducted on execution time, resource consumption, and throughput.
- The framework faces scalability challenges, potential latency issues due to blockchain transaction validation, and the need for further optimisation in integrating IoT devices with blockchain infrastructure for real-time processing.

LITERATURE REVIEW (3/8)

Murari Kumar Singh, Sanjeev Kumar Pippal, Vishnu Sharma, Lightweight blockchain mechanism for secure data transmission in healthcare system, Biomedical Signal Processing and Control, Volume 102, 2025.

- The study presents a lightweight blockchain mechanism for secure data transmission in healthcare systems, addressing challenges like data privacy, interoperability, and security while ensuring efficient access to medical data.
- The proposed model integrates a hybrid security-based minor solution using an optimized consensus algorithm that combines Proof of Work (PoW) and Proof of Stake (PoS) to balance computational efficiency, security, and decentralization in a blockchain framework.
- The study identifies challenges such as scalability limitations, regulatory compliance issues, data integrity concerns, and difficulties in integrating blockchain technology with existing healthcare infrastructures while ensuring minimal computational overhead.

LITERATURE REVIEW (4/8)

Mehar Nasreen, Sunil Kumar Singh, "BPMT: A hybrid model for secure and effective electronic medical record management system", Journal of Computational Science, Volume 83, 2024.

- The study introduces BPMT, a hybrid model integrating Merkle and B+ trees to enhance the security, efficiency, and scalability of blockchain-based EMR management, addressing challenges in data retrieval, storage, and system throughput.
- BPMT leverages B+ trees for efficient record retrieval and Merkle trees for data integrity, optimizing storage, reducing latency, and improving transaction throughput. The model is validated through complexity analysis and testing on multiple datasets.
- Despite performance gains, challenges include increased computational complexity, scalability issues in large deployments, and network latency, requiring further optimization for real-world applications.

LITERATURE REVIEW (5/8)

M. Nankya, A. Mugisa, Y. Usman, A. Upadhyay, and R. Chataut, "Security and Privacy in E-Health Systems: A Review of AI and Machine Learning Techniques", IEEE Access, vol. 12, 2025.

- The paper examines AI and machine learning applications in e-health security, focusing on threat detection, anomaly identification, and predictive analytics to protect sensitive medical data.
- It explores AI-driven cybersecurity approaches such as anomaly detection, automated countermeasures, and adaptive learning, along with privacy-preserving techniques like federated learning, quantum-resistant encryption, and blockchain integration.
- The study highlights challenges including the need for more robust AI models, integration difficulties with existing healthcare systems, and concerns regarding regulatory compliance, ethical considerations, and patient data privacy.

LITERATURE REVIEW (6/8)

Seunghee Lee, Gyun-Ho Roh, Jong-Yeup Kim, Young Ho Lee, Hyekyung Woo, Suehyun Lee, "Effective data quality management for electronic medical record data using SMART DATA", International Journal of Medical Informatics, Volume 180, 2023.

- The study introduces a SMART DATA-based quality management system for electronic medical records (EMRs) to enhance data reliability, reduce errors, and improve the utilization of medical data in clinical research.
- The proposed system follows a three-stage framework (Construction - Operation - Utilization) to manage the EMR data lifecycle. It integrates structured data extraction, semantic information validation, and real-world clinical scenario testing using colorectal cancer datasets to refine predictive modeling.
- The approach faces limitations in scalability, requires further customization for diverse diseases and institutions, and needs more practitioner input to refine its clinical applicability and quality assessment methods.

LITERATURE REVIEW (7/8)

Usha Nicole Cobrado, Suad Sharief, Noven Grace Regahal, Erik Zepka, Minnie Mamauag, Lemuel Clark Velasco, "Access control solutions in electronic health record systems: A systematic review", Informatics in Medicine Unlocked, Volume 49, 2024.

- The study reviews access control solutions in EHR systems, categorizing them into Identification, Authentication, Authorization, and Accountability (IAAA) to enhance security and privacy.
- Following PRISMA 2020 guidelines, it analyzes 20 journal articles, examining access control mechanisms like ABAC, RBAC, and authentication models such as digital signatures and mutual authentication.
- Key challenges include limited multi-factor authentication, lack of emergency access, weak patient consent mechanisms, and difficulties in regulatory compliance, hindering real-world adoption.

LITERATURE REVIEW (8/8)

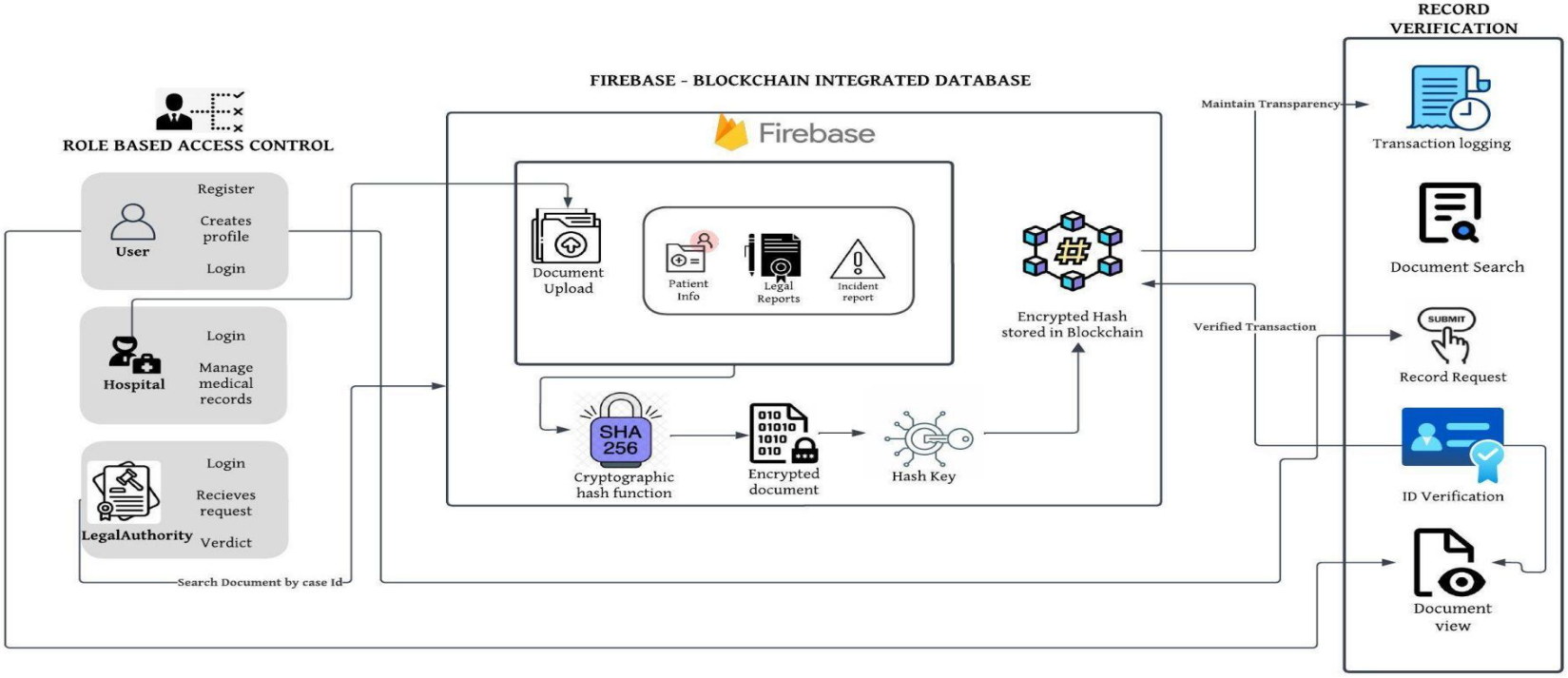
Xiao Qu, Zhexuan Yang, Zeng Chen, Guozi Sun, "A consent-aware electronic medical records sharing method based on blockchain", Computer Standards & Interfaces,Volume 92, 2025.

- The study proposes a consent-aware electronic medical records (EMR) sharing method based on blockchain to enhance data security, privacy, and patient control over medical information.
- The system leverages blockchain for transparency and decentralization, integrates on-chain verification mechanisms to prevent data tampering, and utilizes secure off-chain storage for scalability. Experiments were conducted using Ethereum smart contracts on Ganache and Remix-based networks to validate security and economic feasibility.
- The approach faces scalability concerns due to blockchain's storage constraints, network latency issues, and potential security risks such as 51% attacks and smart contract vulnerabilities, requiring further enhancements in cryptographic defenses.

ISSUES AND CHALLENGES

- Traditional medico-legal record management is inefficient, requiring extensive manpower and increasing the risk of data misplacement and loss.
- Manual handling leads to data loss, errors, and unauthorised access, compromising security.
- Lack of integration delays real-time document verification for hospitals and legal authorities.
- Security risks, including data breaches, highlight the need for encryption and tamper-proof storage.
- Indian Evidence Act, 1872—Sections 3 & 45 ensure medico-legal records are legally admissible, requiring a structured digital system.
- IT Act, 2000 – Section 72 mandates protection of electronic records, ensuring confidentiality and compliance.
- Existing systems lack scalability and interoperability, making large-scale record management inefficient.

ARCHITECTURE DIAGRAM



SYSTEM REQUIREMENTS AND TOOLS

Hardware Requirements:

- **Processor :** Intel Core i7 11th Gen
- **RAM :** 8GB
- **Hard Disk :** 512 GB - 1 TB
- **GPU:** NVIDIA GeForce RTX 3050

Software Requirements :

- **Operating system:** Windows 11
- **Framework :** Flutter
- **Database:** FireBase
- **IDE:** Android Studio
- **Programming language:** Java, DART

MODULES

1. USER AUTHENTICATION & RECORD REQUEST MODULE.
2. HOSPITAL RECORD MANAGEMENT AND ENCRYPTION MODULE.
3. LEGAL AUTHORITY RECORD VERIFICATION AND RETRIEVAL MODULE.
4. FIREBASE AND BLOCKCHAIN-BASED DATA INTEGRITY MODULE.

MODULES DESCRIPTION (1/4)

1. USER AUTHENTICATION & RECORD REQUEST MODULE

- The user module ensures secure access by using Firebase authentication, allowing users to register, log in, and access features based on their roles.
- Every time a user requests or updates a document, a SHA-256 hash is created and stored on the blockchain, making records tamper-proof.
- Users can easily search, request, and retrieve medico-legal records stored securely in Firebase Storage.
- All document interactions are logged on the blockchain, ensuring transparency, security, and compliance with legal standards.
- The system keeps records up to date in real time using Firebase Realtime Database, while blockchain technology helps maintain data integrity.

MODULES DESCRIPTION (2/4)

2. HOSPITAL RECORD MANAGEMENT AND ENCRYPTION MODULE

- The Hospital Record Management Module securely stores and manages patient records using Firebase Realtime Database and Firebase Storage, ensuring quick and efficient access.
- Sensitive medical records, such as case histories and legal documents, are encrypted with SHA-256 before storage to maintain confidentiality.
- Every uploaded document is hashed using SHA-256 and recorded on the blockchain, preventing unauthorized changes and ensuring data integrity.
- Authorized users can search, update, and retrieve hospital records based on their access levels, with logs maintained for transparency and security.
- The system follows strict privacy regulations, ensuring that all data remains protected during storage and transmission.

MODULES DESCRIPTION (3/4)

3. LEGAL AUTHORITY RECORD VERIFICATION AND RETRIEVAL MODULE

- The Legal Authority Record Verification and Retrieval Module enables secure access to medico-legal records through role-based authentication and authorisation.
- Legal authorities can search, request, and retrieve verified records, ensuring compliance with regulatory and legal standards.
- Each document request and modification is logged on the blockchain using SHA-256 hashing, ensuring data integrity and preventing unauthorised alterations.
- Access permissions are strictly enforced, allowing only authorised personnel to view and validate sensitive legal and medical records.
- The system ensures secure document transmission and retrieval while maintaining transparency through detailed audit logs.

MODULES DESCRIPTION (4/4)

4. FIREBASE AND BLOCKCHAIN-BASED DATA INTEGRITY MODULE

- The Firebase and Blockchain-Based Data Integrity Module ensures secure storage, retrieval, and validation of sensitive records through a decentralized and tamper-proof system.
- All records are stored in Firebase Realtime Database and Firebase Storage, with SHA-256 hashing applied to maintain data integrity and prevent unauthorized modifications.
- Each transaction, including document uploads and updates, is recorded on the blockchain, ensuring transparency, traceability, and protection against data breaches.
- Role-based access control restricts unauthorized modifications, while blockchain verification ensures that stored records remain immutable and verifiable.
- The system enhances security and compliance by integrating real-time data validation with blockchain-backed audit trails for legal and regulatory adherence.

IMPLEMENTATION SCREENSHOT (1/9)

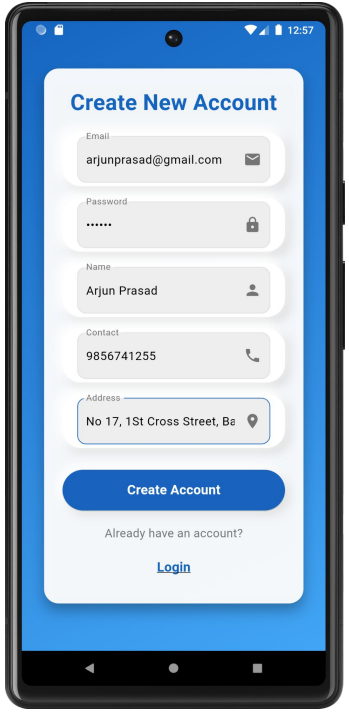


Fig 1.1. User Signup Page

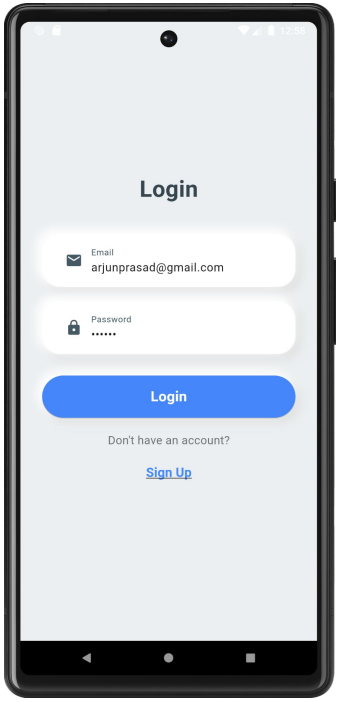


Fig 1.2. User Login Page

Fig 1.3. User Request Page

IMPLEMENTATION SCREENSHOT (2/9)

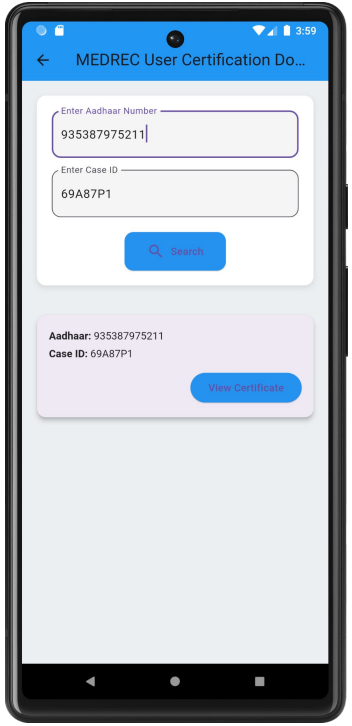


Fig 2.1. User Request Page

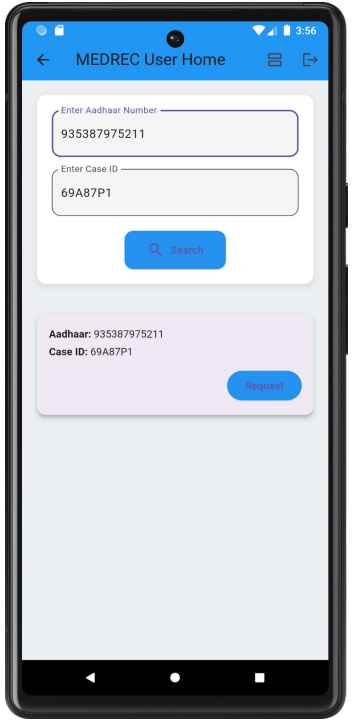


Fig 2.2. User Record View Page

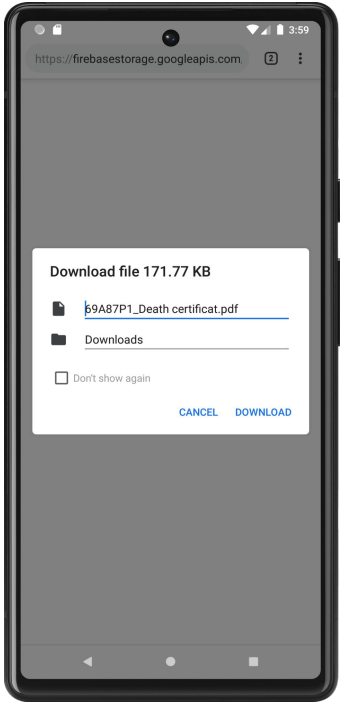


Fig 2.2. User Record Download Page

IMPLEMENTATION SCREENSHOT (3/9)

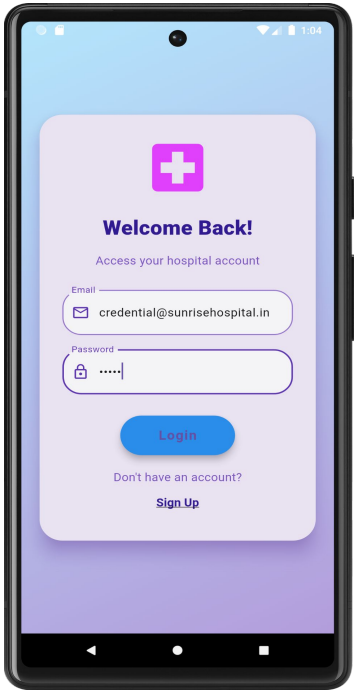


Fig 3.1. Hospital Login Page

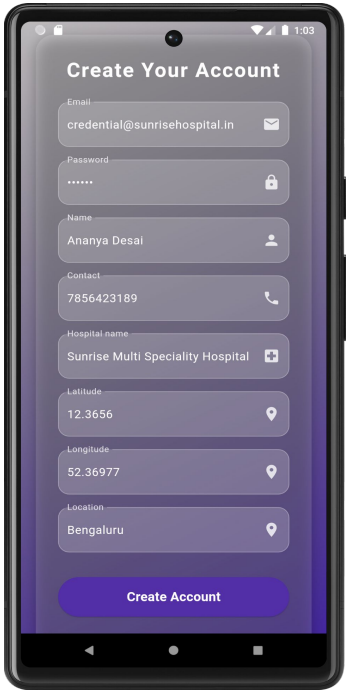


Fig 3.2. Hospital Signup Page

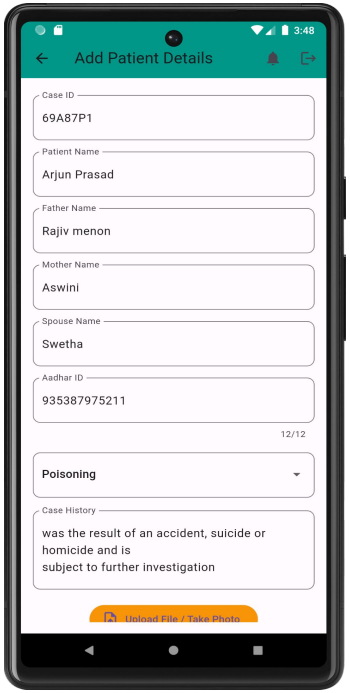


Fig 3.3. Hospital - Patient Register Page

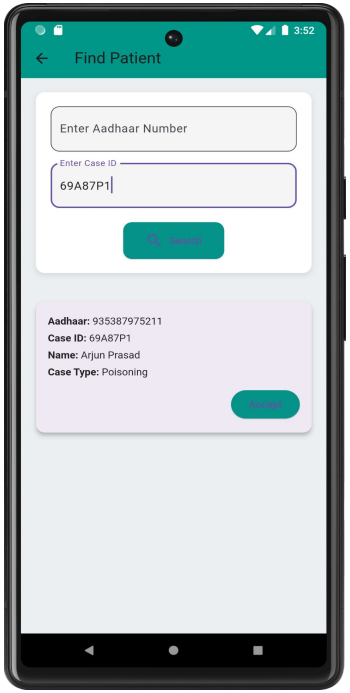


Fig 3.4. Hospital - Patient Record Accept Page

IMPLEMENTATION SCREENSHOT (4/9)

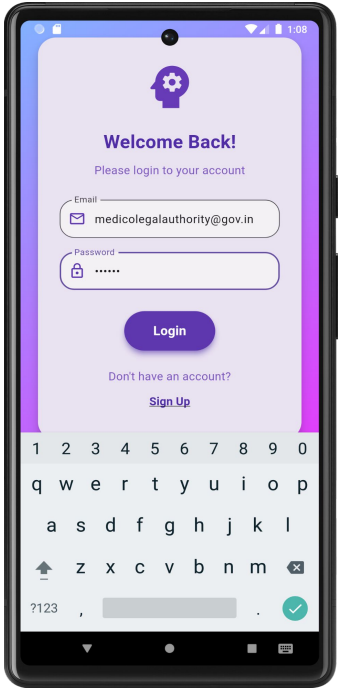


Fig 4.1. Legal Authority Login Page

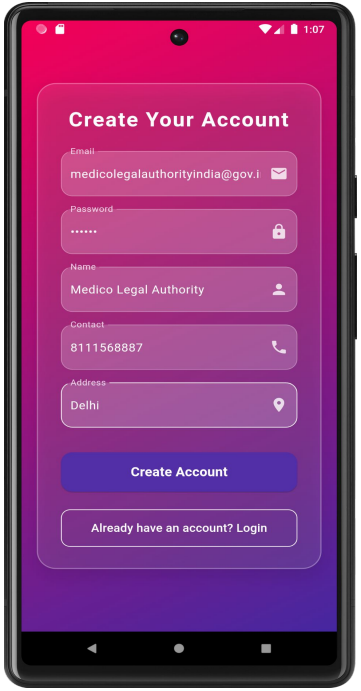


Fig 4.2. Legal Authority Signup Page

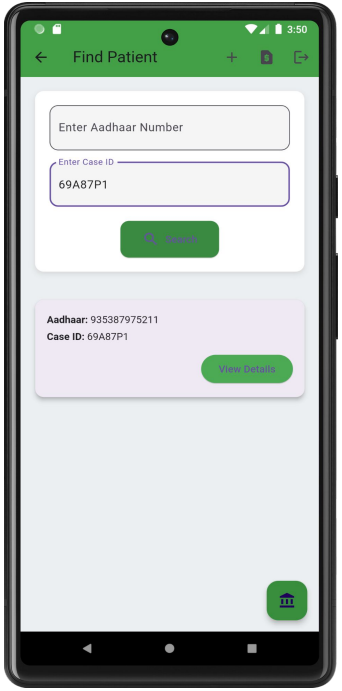


Fig 4.3. Legal Authority Request Search Page

IMPLEMENTATION SCREENSHOT (5/9)

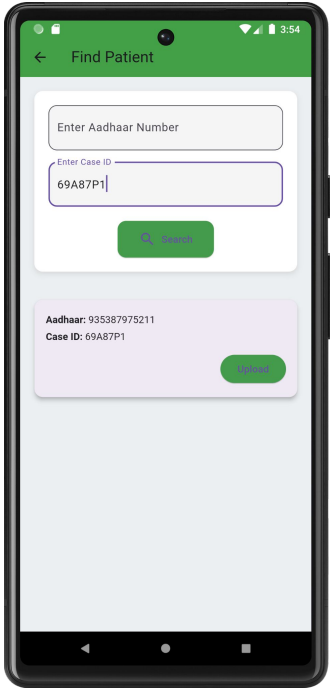


Fig 5.1. Legal Authority Record upload Page

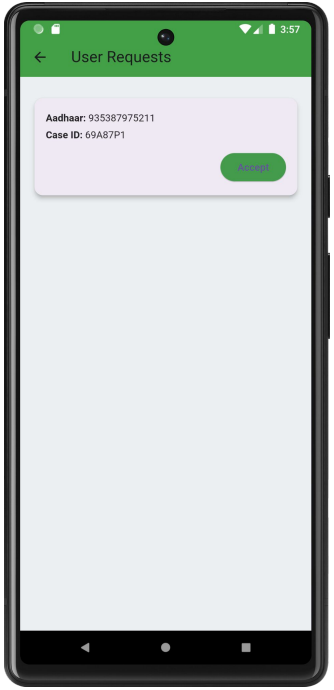


Fig 5.2. Legal Authority user Request Accept Page

IMPLEMENTATION SCREENSHOT (6/9)

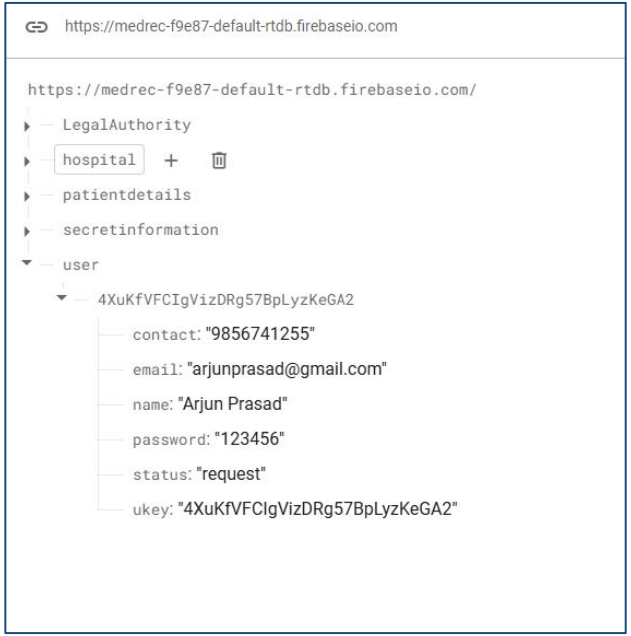


Fig 6.1. Firebase User Credential

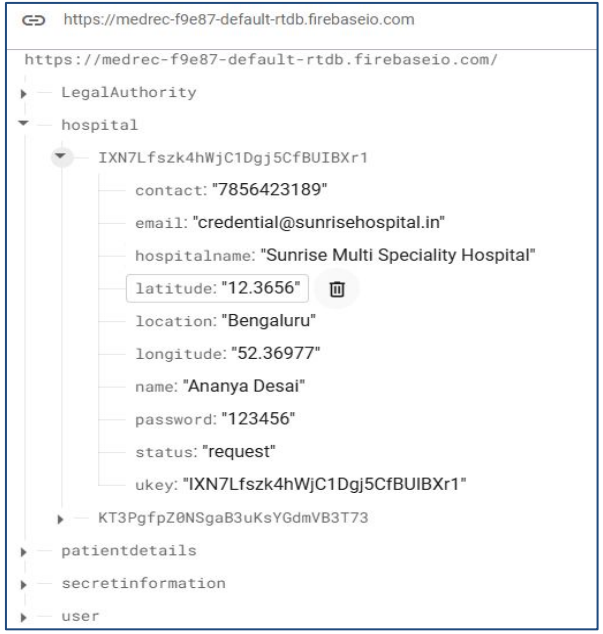


Fig 6.2. Firebase Hospital Credential

Fig 6.3. Firebase Legal Authority Credential

IMPLEMENTATION SCREENSHOT (7/9)

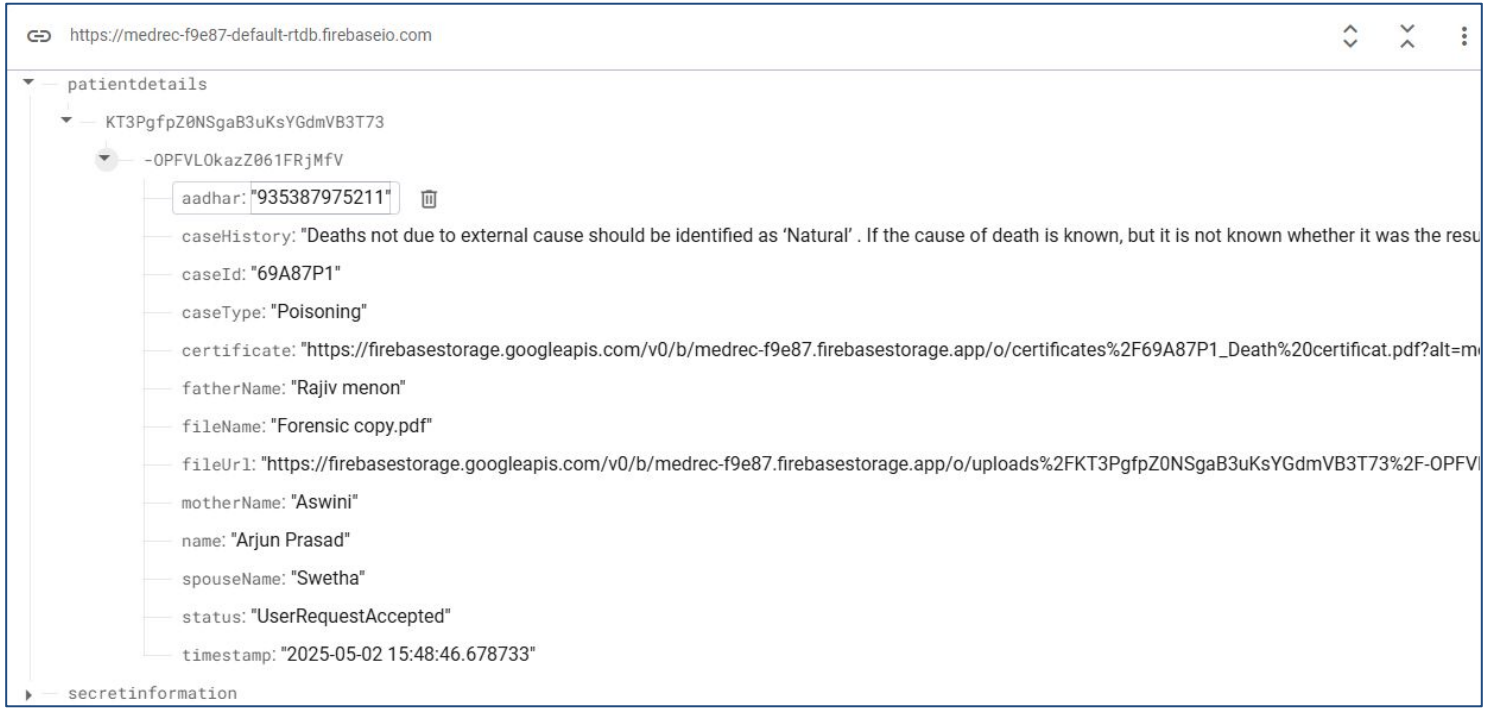
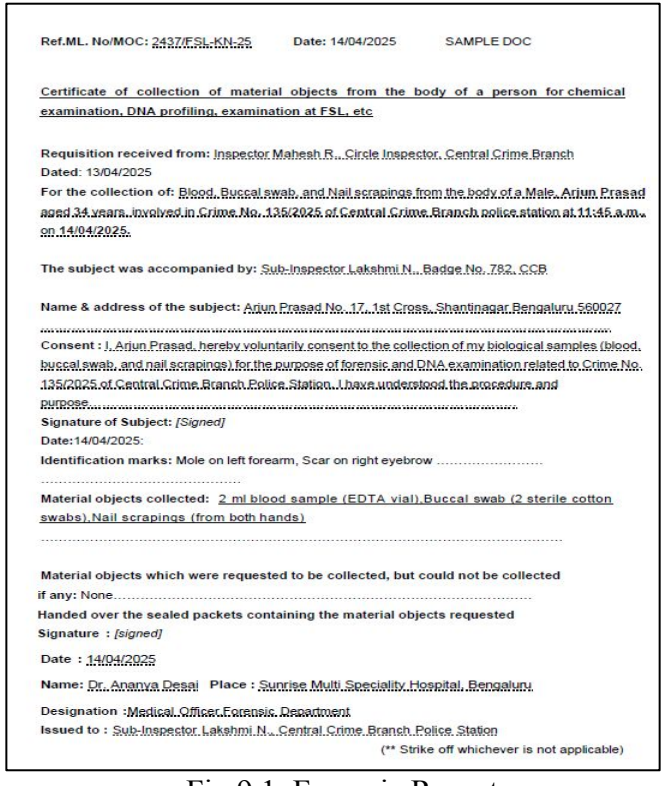


Fig 7.1. Firebase Patient Details

IMPLEMENTATION SCREENSHOT (8/9)

Fig 8.1. Firebase Confidential Information Storage Using SHA-256 Hash Function

IMPLEMENTATION SCREENSHOT (9/9)



Ref.ML. No/MOC: 2437/FSL-KN-25 Date: 14/04/2025 SAMPLE DOC

Certificate of collection of material objects from the body of a person for chemical examination, DNA profiling, examination at FSL, etc

Requisition received from: Inspector Mahesh R., Circle Inspector, Central Crime Branch
Dated: 13/04/2025
For the collection of: Blood, Buccal swab, and Nail scrapings from the body of a Male, Arjun Prasad aged 34 years, involved in Crime No. 135/2025 of Central Crime Branch police station at 11:45 a.m. on 14/04/2025.

The subject was accompanied by: Sub-Inspector Lakshmi N., Badge No. 782, CCB

Name & address of the subject: Arjun Prasad No. 17, 1st Cross, Shantinagar Bengaluru 560027
.....
Consent : I, Arjun Prasad, hereby voluntarily consent to the collection of my biological samples (blood, buccal swab, and nail scrapings) for the purpose of forensic and DNA examination related to Crime No. 135/2025 of Central Crime Branch Police Station. I have understood the procedure and purpose.
Signature of Subject: *[Signed]*
Date:14/04/2025:
Identification marks: Mole on left forearm, Scar on right eyebrow .....
.....
Material objects collected: 2 ml blood sample (EDTA vial),Buccal swab (2 sterile cotton swabs),Nail scrapings (from both hands)
.....

Material objects which were requested to be collected, but could not be collected if any: None.....
Handed over the sealed packets containing the material objects requested
Signature : *[signed]*

Date : 14/04/2025

Name: Dr. Ananya Desai Place : Sunrise Multi Speciality Hospital, Bengaluru

Designation :Medical Officer,Forensic Department
Issued to : Sub-Inspector Lakshmi N., Central Crime Branch Police Station

(** Strike off whichever is not applicable)

Fig 9.1. Forensic Report

REFERENCES

1. Abeer Z. Al-Marridi, Amr Mohamed, Aiman Erbad, Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning, Journal of Network and Computer Applications, Volume 224, 2024.
2. Alessandra Rizzardi, Sabrina Sicari, Jesus F. Cevallos M., Alberto Coen-Porisini, IoT-driven blockchain to manage the healthcare supply chain and protect medical records, Future Generation Computer Systems, Volume 161, 2024.
3. Murari Kumar Singh, Sanjeev Kumar Pippal, Vishnu Sharma, Lightweight blockchain mechanism for secure data transmission in healthcare system, Biomedical Signal Processing and Control, Volume 102, 2025.
4. Mehar Nasreen, Sunil Kumar Singh, “BPMT: A hybrid model for secure and effective electronic medical record management system”, Journal of Computational Science, Volume 83, 2024.

REFERENCES

5. M. Nankya, A. Mugisa, Y. Usman, A. Upadhyay, and R. Chataut, “Security and Privacy in E-Health Systems: A Review of AI and Machine Learning Techniques”, IEEE Access, vol. 12, 2025.

6. Seunghee Lee, Gyun-Ho Roh, Jong-Yeup Kim, Young Ho Lee, Hyekyung Woo, Suehyun Lee, “Effective data quality management for electronic medical record data using SMART DATA”, International Journal of Medical Informatics, Volume 180, 2023.

7. Usha Nicole Cobrado, Suad Sharief, Noven Grace Regahal, Erik Zepka, Minnie Mamauag, Lemuel Clark Velasco, “Access control solutions in electronic health record systems: A systematic review”, Informatics in Medicine Unlocked, Volume 49, 2024.

8. Xiao Qu, Zhexuan Yang, Zeng Chen, Guozi Sun, “A consent-aware electronic medical records sharing method based on blockchain”, Computer Standards & Interfaces,Volume 92, 2025.