



GoldenTime: A Blockchain-Based Decentralized Medical Identity And Emergency Response System

Akshay A D¹, Kiran K P², Mahendra M³, Marula Kumar D S⁴, Guide : Ms. Deepti H G⁵

¹⁻⁴ Department of Computer Science and Engineering, GM Institute of Technology, Davanagere, Karnataka, India

⁵ Department of Computer Science and Engineering, G M University, Davanagere, Karnataka, India

E-mail: akshaydappadule18@gmail.com, kirankatare158@gmail.com, mahendram7892@gmail.com, manusmarty61@gmail.com, deeptihg.fet.scst@gmu.ac.in

ABSTRACT :

Healthcare data management faces significant challenges including fragmented records, risk of unauthorized modification, and critical delays during medical emergencies. GoldenTime is a blockchain-integrated medical record management system built on the MERN stack and Ethereum smart contracts that addresses these challenges. The system introduces a dual-tier data model where non-confidential emergency data such as blood group and allergies are publicly accessible via a QR-based Emergency Grid, while confidential records are exposed only through contract functions restricted to on-chain authorized doctors. A Solidity smart contract named GoldenTimeLedgerV3 serves as the immutable data layer, enforcing role-based access through the onlyAuthorized modifier. The backend is implemented using Node.js and Express.js with MongoDB for off-chain mirroring, Cloudinary for file storage, and Nodemailer for OTP-based two-factor authentication. The frontend is built with React 19 and Ethers.js v6 for direct blockchain interaction. The system was deployed and tested on the Ethereum Sepolia test network. Results demonstrate tamper-proof record storage, instant emergency data retrieval without authentication, and a complete doctor credential verification workflow.

Keywords: blockchain; healthcare; Ethereum; smart contract; electronic health records; QR code; MERN stack; decentralized; emergency access; Solidity

Introduction

Healthcare data management is one of the most critical problems in modern digital infrastructure. Patient medical records are often scattered across multiple hospital databases, making it difficult for doctors and emergency responders to access complete and accurate information quickly. Traditional Electronic Health Record (EHR) systems are centralized, which makes them vulnerable to data tampering, unauthorized modification, and single points of failure (Tariq et al., 2025).

A particularly severe consequence of this fragmentation occurs during the Golden Hour, the critical window immediately following a traumatic injury or medical emergency in which prompt treatment is most likely to prevent death or permanent disability. During this period, delays in retrieving a patient's blood group or known allergies can lead to treatment errors.

GoldenTime is a blockchain-integrated healthcare data management system designed to solve these problems. The system stores medical records on an Ethereum-based smart contract, making them immutable and verifiable. A QR-based Emergency Grid enables paramedics and first responders to retrieve critical patient information instantly, without any login or authentication. Role-based access control enforced by the smart contract ensures that only verified and admin-approved doctors can write patient records.

This paper presents the architecture, implementation, and results of the GoldenTime system, covering the smart contract design, backend REST API, frontend dashboards, and the Emergency QR access mechanism.

Literature survey

Tariq et al. (2025) presented a systematic literature review of blockchain for secure healthcare data sharing, published in IEEE Access. The review concludes that blockchain has significant potential for securing health data sharing, while limitations remain in blockchain-based access control systems. Divyashree and Ravi (2024) present a comprehensive review of blockchain-based secure EHRs, addressing challenges and opportunities in healthcare

data management. Ramzan et al. (2023) discuss the motivations and challenges of healthcare applications that use blockchain technology.

Several studies focus on the security and privacy of electronic health records (EHRs). Hamela et al. (2024) study data security and privacy in EHRs with blockchain and report that blockchain improves the dependability and security of EHR data, while technology maturity, resource allocation, and cost remain obstacles. Rudrakar et al. (2025) discuss blockchain innovation for healthcare data security, with smart contracts and interoperability among the topics covered. Utami et al. (2025) study blockchain for securing EHRs and enhancing data privacy, noting scalability and regulatory issues. Devi et al. (2023) address healthcare data security using blockchain, considering consensus mechanisms such as proof of stake and delegated proof of stake.

Other work targets patient-centric data exchange, identity, and access control. Khatiwada et al. (2022) present a reference design model for a patient-centric healthcare data exchange environment, with emphasis on patient control of health data and security. Chouhan et al. (2025) propose blockchain-based decentralized identifiers for entity authentication in EHRs, with a patient-centric focus on identity and access management. Guo et al. (2023) propose a hybrid blockchain-edge architecture for EHR management that uses attribute-based signature aggregation, attribute-based encryption, and homomorphic encryption.

These works establish blockchain as a means of improving the security, privacy, and decentralization of health records. GoldenTime builds on this direction and focuses specifically on a dual-tier data model with a public QR-based emergency tier, an admin-approved doctor verification workflow with OTP-based two-factor login, and smart-contract-enforced role-based write access. Compared with encryption-based designs such as that of Guo et al. (2023), GoldenTime favors simplicity and fast emergency access, and lists encryption of confidential entries as future work.

System architecture

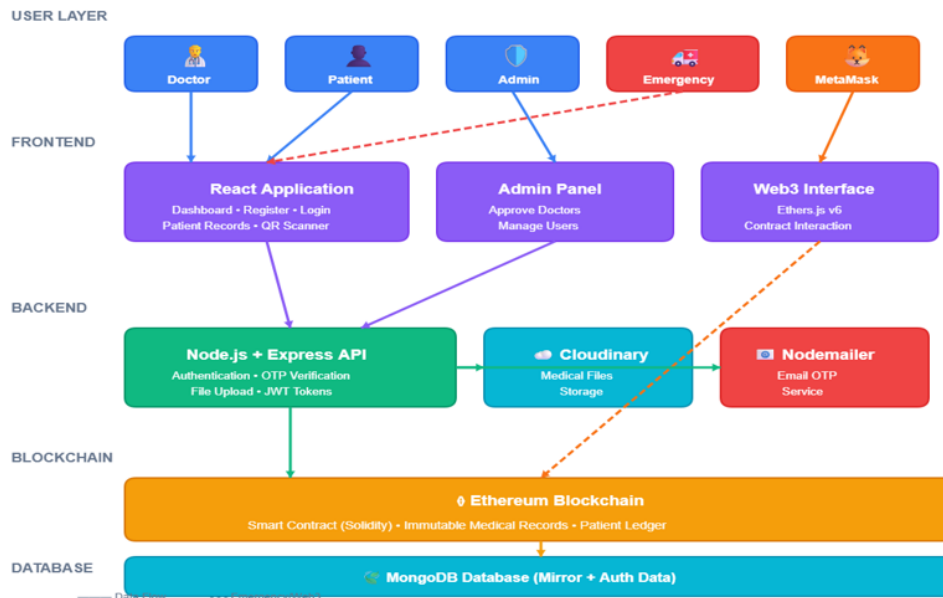


Fig. 1. GoldenTime system architecture showing three-layer design.

GoldenTime follows a three-layer architecture with clear separation of concerns, as shown in Fig. 1.

Blockchain layer The smart contract *GoldenTimeLedgerV3*, written in Solidity (version 0.8.19), is the authoritative and immutable data layer. It defines three core data structures:

- Provider: Stores doctor name, licence number, and authorization status.
- PatientProfile: Stores patient ID (uint256), phone, email, and wallet address.
- MedicalEntry: Stores diagnosis key, value, description, prescription, isConfidential flag, author wallet, author name, and Unix timestamp.

Cross-reference mappings (phoneToId, emailToId, walletToId) enable flexible patient lookup. The onlyAuthorized modifier ensures only admin-approved wallets can write records.

Backend layer The backend is implemented using *Node.js* (v18+) and *Express.js* (v5.2.1). It handles:

- Doctor registration with Cloudinary file upload for credentials

- OTP generation and delivery via Nodemailer (Gmail)
- JWT-based authentication (24-hour validity)
- Patient QR code generation using the qrcode npm package
- MongoDB data mirroring via Mongoose (v9.2.1)

3.3 Frontend layer

The frontend is built with React 19 and Vite (v7.3.1). It provides three role-based dashboards for Admin, Doctor, and Patient. Ethers.js v6 enables direct browser-to-blockchain interaction. The HTML5-QRCode library handles real-time QR code scanning. (1)

4. Implementation

4.1. Smart contract design

The GoldenTimeLedgerV3 contract exposes two access paths for medical data. The public function `getPrimaryData(patientID)` returns only non-confidential entries such as blood group, allergies, and emergency contacts, with no authentication. The function `getFullMedicalHistory(patientID)` is restricted by the `onlyAuthorized` modifier and returns the complete history, including diagnoses and prescriptions. Authorized doctors add patients with `onboardPatient()` and append records with `updatePatientData()`, and both operations emit events for off-chain indexing.

4.2. Doctor registration and authentication

A doctor registers with personal details, wallet address, licence ID, and certificate images, as shown in Fig. 2. The backend uploads the images to Cloudinary and stores the URLs in MongoDB with status "pending". Login uses two factors: the registered email with MetaMask wallet address, followed by a 6-digit OTP sent through Nodemailer with a 10-minute expiry. A successful verification returns a JWT valid for 24 hours.

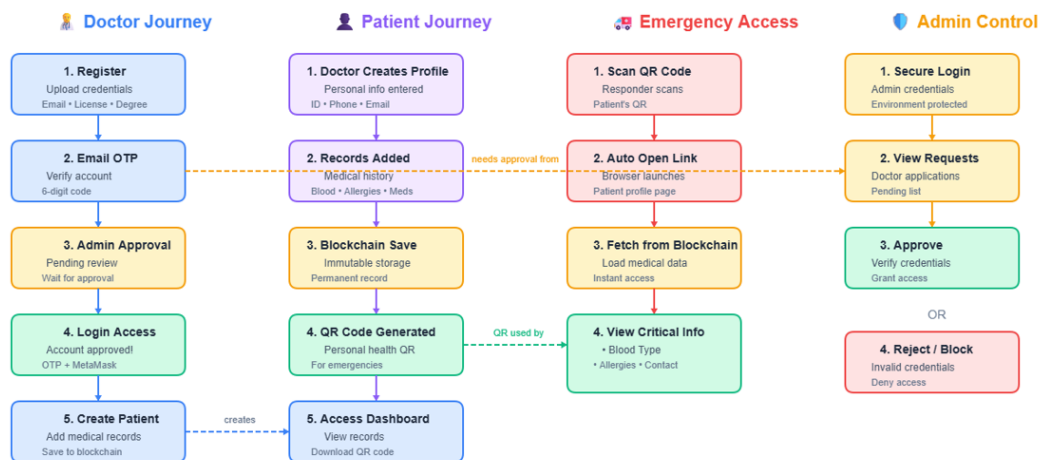


Fig. 2 - Full system flowchart covering registration, login, onboarding, and access paths.

4.3. Patient onboarding and emergency QR access

When a doctor onboards a patient, the frontend calls `onboardPatient()` through Ethers.js and calls the backend `/api/patient/sync` endpoint in parallel. The backend generates a QR code encoding the patient's page URL and stores it in MongoDB for printing. When a responder scans the QR code, the frontend calls `getPrimaryData(patientID)`, a public view function that needs no login, wallet, or gas, and displays the emergency data instantly.

4.4. Admin and doctor dashboards

The admin dashboard (Fig. 3) lists registered doctors and lets the admin approve, reject, or block them. Approved doctors are then authorized on-chain through `authorizeProvider()`. The doctor dashboard (Fig. 4) provides patient onboarding, search by phone, email, or wallet address, and record updates. All write transactions are signed in MetaMask, and the `onlyAuthorized` modifier rejects unauthorized wallets.

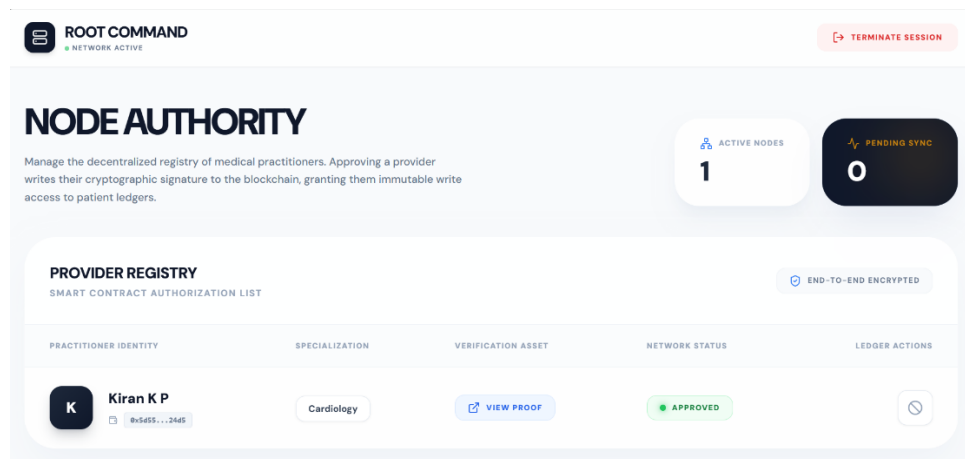


Fig. 3 - Admin dashboard showing doctor credential review and approval controls.

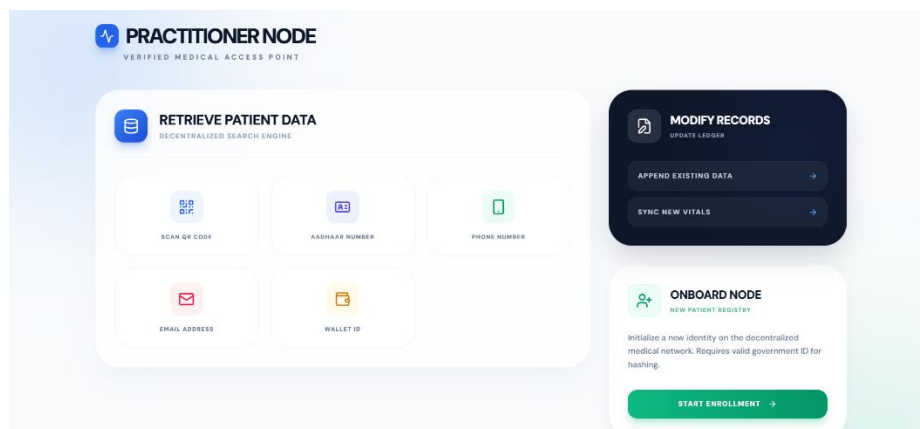


Fig. 4 - Doctor dashboard showing patient search and record management interface.

5. Results

5.1. Functional testing

All major system features were tested end-to-end on the Ethereum Sepolia test network. Doctor registration, admin approval, OTP login, patient onboarding on-chain, QR generation, medical record updates, emergency QR scanning, and patient dashboard access all produced correct and expected results. The onlyAuthorized modifier successfully rejected all unauthorized wallet write attempts with a contract-level revert.

5.2. Blockchain behaviour

Patient onboarding transactions were confirmed on the Sepolia test network. The getPrimaryData() function is a read-only view call, so it requires no gas and no wallet connection, which makes it suitable for emergency use. All cross-reference lookups (phoneToId, emailToId, walletToId) returned correct patient IDs for all test inputs.

5.3. Security testing

Blocked doctor accounts received a 403 Forbidden response on login. Pending accounts were correctly denied access. Expired JWT tokens (beyond 24 hours) were rejected by protected API routes. Expired OTPs (beyond 10 minutes) were invalidated correctly. Confidential records were confirmed as completely hidden from the public getPrimaryData() response. The API endpoint results are summarized in Table 1.

Table 1 - API endpoint test results.

Endpoint	Method	Result
/api/doctor/register	POST	200 OK
/api/doctor/login	POST	200 OK
/api/doctor/verify-otp	POST	200 OK
/api/admin/login	POST	200 OK
/api/admin/doctors	GET	200 OK
/api/admin/change-status	POST	200 OK
/api/admin/toggle-block	POST	200 OK
/api/patient/sync	POST	200 OK
/api/patient/qr	GET	200 OK

6. Applications

GoldenTime has potential applications across several healthcare scenarios. In emergency medical services, paramedics can scan the patient QR code to retrieve blood group, allergies, and emergency contacts without requiring any authentication. In multi-hospital networks, patients who visit multiple hospitals can have their records consolidated under a single blockchain identity, reducing duplicate tests and conflicting prescriptions. Immutable on-chain records could also serve as tamper-evident support in insurance claims, and printed QR cards could help identify patients in areas with limited connectivity.

7. Conclusion and future work

This paper presented GoldenTime, a decentralized medical identity and emergency response system that combines Ethereum smart contracts, MetaMask authentication, off-chain Cloudinary storage, and QR-based retrieval. The system gives patients ownership of their records, protects data integrity through on-chain records, and shortens the time responders need to reach critical information.

Future work includes encrypting confidential entries, adding biometric authentication, deploying on a low-cost Layer-2 network, supporting offline emergency access, integrating with hospital information systems, and testing with real users at larger scale.

Acknowledgements

The authors thank the Department of Computer Science and Engineering, GM Institute of Technology, Davanagere, for their guidance and support.

REFERENCES

1. Chouhan, G. K., Singh, S., Jaduvansy, A., Rai, P., & Rath, A. (2025). A blockchain based decentralized identifiers for entity authentication in electronic health records. *Proc. 2025 Int. Conf. Intelligent and Cloud Computing (ICoICC)*, 1–6. <https://doi.org/10.1109/ICoICC64033.2025.11052007>
2. Devi, T., Kamatchi, S. B., & Deepa, N. (2023). Enhancing the security for healthcare data using blockchain technology. *Proc. 2023 Int. Conf. Computer Communication and Informatics (ICCCI)*, 1–7. <https://doi.org/10.1109/ICCCI56745.2023.10128545>
3. Divyashree, D., & Ravi, C. (2024). A comprehensive review of blockchain based secure EHR: Addressing challenges and unlocking opportunities in healthcare data management. *Proc. 2024 3rd Int. Conf. Innovation in Technology (INOCON)*, 1–6. <https://doi.org/10.1109/INOCON60754.2024.10511953>
4. Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2023). A hybrid blockchain-edge architecture for electronic health record management with attribute-based cryptographic mechanisms. *IEEE Transactions on Network and Service Management*, 20(2), 1759–1774. <https://doi.org/10.1109/TNSM.2022.3186006>

5. Hamela, K., Shrivastava, G., Umapathi, P., Bankar, J. S., Chaudhary, S. D., & Kisan, R. (2024). Enhancing data security and privacy in electronic health records with blockchain technology. *Proc. 2024 4th Int. Conf. Technological Advancements in Computational Sciences (ICTACS)*, 1829–1835. <https://doi.org/10.1109/ICTACS62700.2024.10841078>
6. Khatiwada, P., Yang, B., & Skjelvik, A. (2022). Reference design model for a patient-centric data exchange healthcare environment. *Proc. 2022 3rd Int. Conf. Human-Centric Smart Environments for Health and Well-being (IHSH)*, 49–56. <https://doi.org/10.1109/IHSH57076.2022.10092114>
7. Ramzan, S., Aqduş, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2023). Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management*, 70(8), 2874–2890. <https://doi.org/10.1109/TEM.2022.3189734>
8. Rudrakar, R., Puri, C., Lichade, A., & Shiralaskar, H. (2025). Blockchain innovation for healthcare data security. *Proc. 2025 2nd Int. Conf. Electronic Circuits and Signaling Technologies (ICECST)*, 1138–1143. <https://doi.org/10.1109/ICECST66106.2025.11307662>
9. Tariq, U. U., Sabrina, F., Rashid, M. M., Gordon, S., Lin, Y., Wang, Z., & Azad, S. (2025). Blockchain-based secured data sharing in healthcare: A systematic literature review. *IEEE Access*, 13, 45415–45435. <https://doi.org/10.1109/ACCESS.2025.3547953>
10. Utami, R. T., Lubis, V. H., Royani, Santoso, N. P. L., Rizky, A., Komara, M. A., & Suryadi, L. (2025). Blockchain technology for securing electronic health records and enhancing data privacy. *Proc. 2025 4th Int. Conf. Creative Communication and Innovative Technology (ICCIT)*, 1–7. <https://doi.org/10.1109/ICCIT65724.2025.11167542>