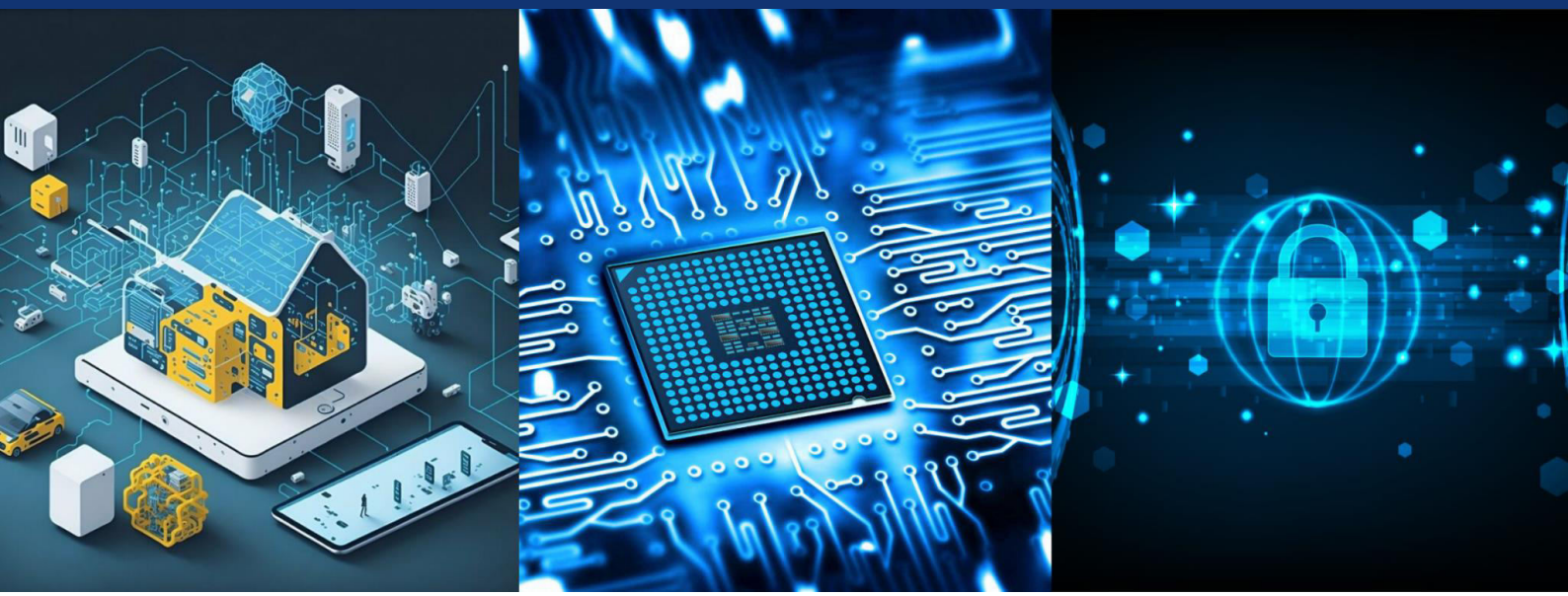
IJIRCCE

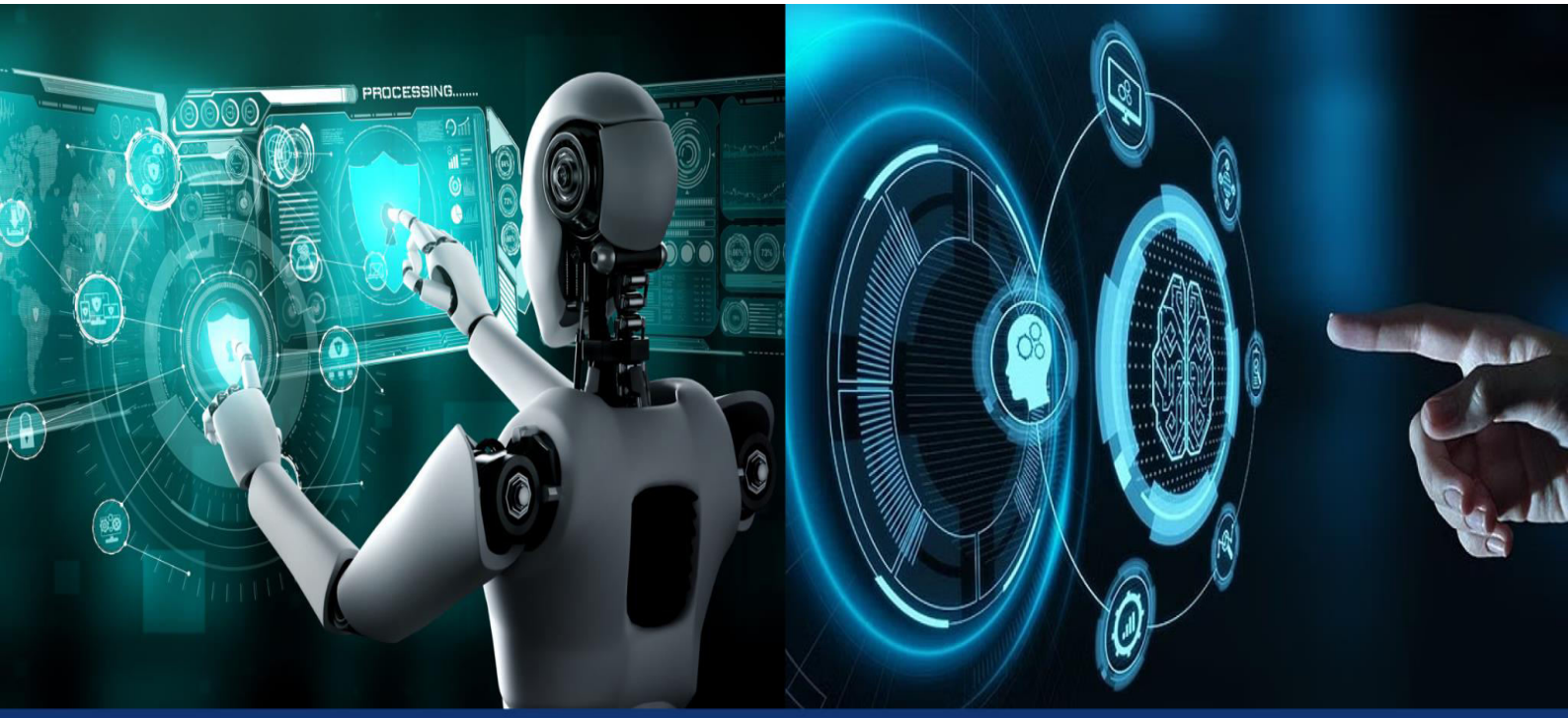
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 7, July 2026

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Online Anonymous Medical Service System Using Blockchain

Janamoni Shyamala, Dr. M. Dhanalakshmi

Post Graduate Student, Department of Computer Science and Engineering(CNIS), Jawaharlal Nehru Technological University, Hyderabad, India

Professor, Department of Computer Science and Engineering, Jawaharlal Nehru Technological University, Hyderabad, India

ABSTRACT: Contemporary telemedicine platforms require patients to register with personal credentials — names, phone numbers, and email addresses — stored on centralized servers that remain exposed to data breaches and regulatory compulsion. This creates a structural privacy gap that discourages patients with sensitive conditions from seeking timely medical care. To overcome these limitations, this study presents an Online Anonymous Medical Service System built on the Solana blockchain that eliminates this gap through three coordinated mechanisms: wallet-only identity, client-side AES encryption, and on-chain consultation state maintained through Anchor Program Derived Accounts (PDAs).

Patients connect a Phantom wallet on Solana Devnet and use their cryptographic public key as their sole system identity. Before any network transmission, medical reports are encrypted in the browser using AES symmetric encryption, ensuring that neither the storage network nor the service provider ever receives plaintext patient data. Encrypted ciphertexts are uploaded to the InterPlanetary File System (IPFS) via the Pinata pinning service. An Anchor smart contract maintains PDAs recording only the consultation ID, encrypted report CID, payment verification status, and encrypted prescription CID — with no personal identifiers at any system layer. Consultation fees are paid in Devnet SOL through Phantom and verified on-chain, doctors interact through an anonymous dashboard, and patients retrieve and locally decrypt prescriptions in the browser so that decryption keys never leave the patient device. Experimental results demonstrate successful end-to-end anonymous consultation flows, on-chain payment confirmation, multi-consultation tracking, and local decryption of prescriptions. The system satisfies a weak-fairness property: either both patient and doctor receive their expected deliverable, or neither does, with the blockchain providing an immutable audit trail.

KEYWORDS: Blockchain, Solana, Anonymous Healthcare, IPFS, AES Encryption, Anchor Smart Contract, Privacy-Preserving, Phantom Wallet, Program Derived Address, Fair Exchange, Decentralized Storage.

I. INTRODUCTION

Healthcare systems across the world are adopting digital consultation platforms that allow patients to interact with physicians remotely. While this transformation improves access to care, it introduces a structural privacy vulnerability: every existing platform requires patients to register with personal identifiers — name, date of birth, phone number, and email address — stored on servers controlled by third parties. These repositories become targets for cyber attacks, and their administrators are subject to legal orders that may compel disclosure. Patients who most need privacy — those seeking advice on stigmatised conditions, whistleblowers, or individuals in exposed public roles — are consequently deterred from using the very systems meant to help them.

Regulatory frameworks including HIPAA in the United States and GDPR in Europe impose a data-minimization principle: service providers must collect only the personal data strictly necessary for the service. A system that delivers a prescription in response to an encrypted medical report, with no personal identifiers at any layer, satisfies this principle more completely than any system that merely promises to protect the personal data it collects. Patient distrust arising from privacy concerns has been documented to reduce adoption of electronic medical records and to cause patients to withhold medically relevant information from providers.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

To address these challenges, this paper proposes an Online Anonymous Medical Service System (CuraCipher) that achieves the same clinical outcome as conventional telemedicine — delivering a physician prescription in response to a patient medical report — without collecting any personal data. The system is built on three technical pillars: patients are identified solely by their Solana blockchain wallet address; medical reports are AES-encrypted inside the browser before any data leaves the patient device; and an Anchor smart contract stores only encrypted IPFS content identifiers and payment flags inside Program Derived Accounts. Providing medical services anonymously also creates a bilateral risk problem — the classic fair-exchange problem — which the system resolves through the Solana blockchain, which records each protocol step immutably and provides non-repudiable proofs of payment and service completion. Experimental results demonstrate that the proposed system functions correctly end-to-end on a live public test network deployment.

II. RELATED WORK

Blockchain-based provision of privacy-sensitive services has been an active research direction. Baranski, Szymanski, and Mora proposed a protocol for anonymous provision of privacy-sensitive services that combines Ethereum as a tamper-proof message board, Monero for anonymous payment, and IPFS/Filecoin for decentralized storage, framing the customer–provider interaction as a fair-exchange problem and proving weak fairness through a game-theoretic model. AlTawy et al. presented Lelantos, a blockchain-based anonymous physical delivery system that demonstrates smart contracts can enforce delivery protocol steps without a trusted intermediary, although it lacks a dispute-resolution mechanism. Hinarejos et al. demonstrated that a public blockchain can replace a trusted third party for certified electronic mail delivery, establishing that blockchain-based non-repudiation is both practical and scalable.

In the healthcare domain, Jin et al. surveyed secure and privacy-preserving medical data sharing and concluded that client-side encryption before storage is the most robust approach against both external adversaries and insider threats at storage providers. Keshta and Odeh identified unauthorized access, data breaches, and lack of patient control over records as the principal challenges in electronic health records. Naresh and Thamarai recommended architectural designs that minimize the collection of identifiable data from the outset rather than applying anonymization as a post-processing step. Despite these advancements, existing telemedicine platforms continue to bind consultations to verified real-world identities and centralized plaintext storage. To overcome these limitations, the proposed framework adapts the fair-exchange, three-layer architecture to a fully online healthcare consultation context on Solana, integrating wallet-only identity, browser-side AES encryption, IPFS content addressing, and smart-contract-enforced consultation state. This combination provides a privacy-preserving and verifiable approach to anonymous medical service delivery.

III. PROPOSED ALGORITHM

A. System Architecture:

The proposed system is organized into four cooperating layers. The Frontend layer (Next.js 14) renders the patient dashboard, doctor dashboard, and patient inbox, and performs all client-side AES encryption and decryption. The Wallet and Payment layer (Phantom / @solana/web3.js) signs transactions and interacts with Solana Devnet RPC nodes. The Blockchain layer (Anchor smart contract on Solana Devnet) maintains consultation PDAs and enforces the protocol state machine. The Storage layer (Pinata IPFS) stores encrypted medical documents and prescriptions as content-addressed immutable objects.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

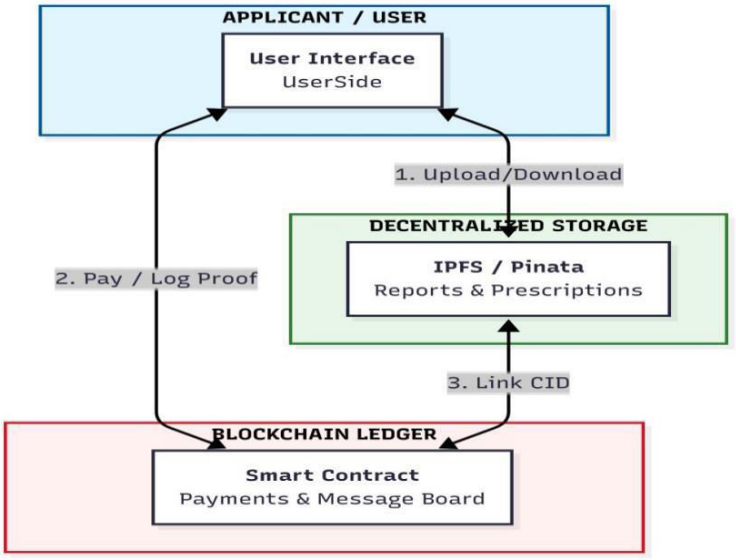


Fig. 1. Proposed System Architecture

B. Design Considerations:

- The system allows patients to connect a Phantom wallet on Solana Devnet and use their public key as sole identity, without collecting any personal information.
- All medical report files are encrypted using AES symmetric encryption entirely within the browser before any network transmission; encryption keys are never transmitted to any server.
- Encrypted report ciphertexts are uploaded to IPFS via the Pinata pinning service, which returns a content identifier (CID) and guarantees content availability throughout the consultation lifecycle.
- An Anchor smart contract creates a consultation PDA storing the consultation ID, encrypted report CID, patient wallet address, payment verification flag, and consultation status.
- Consultation fees are transferred as Devnet SOL from the patient wallet to the doctor wallet, and every payment and state change produces a publicly verifiable on-chain transaction signature.
- Doctors interact through an anonymous dashboard identified only by a generated wallet-derived alias, upload encrypted prescriptions, and mark consultations Completed on-chain.
- The framework provides a patient inbox listing all consultations linked to the connected wallet, with local browser-side download and decryption of prescriptions.

C. Description of the Proposed Algorithm:

The proposed framework aims to deliver an anonymous, verifiable medical consultation using a combination of wallet-based identity, client-side encryption, decentralized storage, and smart-contract state enforcement. The consultation process consists of five major stages.

Step 1: Wallet-Based Anonymous Identity:

The patient connects a Phantom wallet on Solana Devnet. The Ed25519 public key of the wallet serves as the sole system identity; no name, phone number, or email address is ever requested or stored.

$Identity(P) = PubKey(Wallet_p)$ Eq. (1)

where Identity(P) denotes the system identity of patient P. A short display alias is derived from the public key purely for user-interface purposes.

Step 2: Client-Side AES Encryption:

When the patient selects a medical report M, the browser encrypts it with AES symmetric encryption before any network transmission.

$C = AES\_Encrypt(K, M)$ Eq. (2)

where C is the ciphertext and K is the encryption key, which never leaves the patient device. Neither the storage network nor the service provider ever receives plaintext patient data.

Step 3: Decentralized Storage on IPFS:

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The ciphertext is uploaded to the InterPlanetary File System via the Pinata pinning service, which returns an immutable content identifier.

$CID = IPFS\_Store(C)$ Eq. (3)

The CID cryptographically commits to the encrypted content: any modification of the stored document changes its CID, making tampering detectable.

Step 4: On-Chain Consultation State via PDA:

The patient invokes the Anchor smart contract to create a consultation Program Derived Account, which records the consultation state on-chain.

$PDA = Derive(\text{“consultation”}, PubKey(P), ConsultationID)$ Eq. (4)

The PDA stores the patient public key, consultation ID, encrypted report CID, payment verification flag, consultation status, and (later) the encrypted prescription CID. The consultation status follows a strict state machine: Created → Paid → Completed. The patient then transfers the consultation fee in Devnet SOL through Phantom, and the contract verifies the payment and marks the PDA as Paid.

Step 5: Prescription Delivery and Local Decryption:

The doctor reviews the paid consultation through the anonymous dashboard, encrypts and uploads a prescription to IPFS, and calls the contract to store the prescription CID. The smart contract guard requires the payment flag to be true before this instruction succeeds, then sets the status to Completed.

$M' = AES\_Decrypt(K, IPFS\_Fetch(CID_{rx}))$ Eq. (5)

The patient opens the inbox, fetches the encrypted prescription by its CID, and decrypts it locally in the browser to recover the plaintext prescription M′. This adaptive, cryptographically enforced workflow guarantees weak fairness — either both parties receive their expected deliverable or neither does — while the blockchain provides an immutable, publicly verifiable audit trail with no personal identifiers at any layer.

IV. PSEUDO CODE

Step 1: Patient connects the Phantom wallet on Solana Devnet.
Step 2: Obtain the wallet public key and derive an anonymous display alias; query the Devnet RPC for the SOL balance (request an airdrop if the balance is zero).
Step 3: Patient selects a medical report file from the local device.
Step 4: Read the file as an ArrayBuffer in the browser.
Step 5: Encrypt the file with AES using the browser-held key (no key material transmitted).
Step 6: Upload the encrypted blob to IPFS via the Pinata service and receive report CID.
Step 7: Generate a unique timestamp-based consultation ID.
Step 8: Invoke createConsultation(consultationId, reportCid) on the Anchor smart contract to derive and initialize the consultation PDA with status Created.
Step 9: Transfer the consultation fee in Devnet SOL from the patient wallet to the doctor wallet through Phantom.
Step 10: Invoke verifyPayment() on the smart contract.
IF payment transaction is confirmed on-chain
    Set payment_verified ← true; Status ← Paid
ELSE
    Reject the state transition and retain status Created
Step 11: Doctor opens the anonymous dashboard and fetches all Paid consultations.
Step 12: Doctor optionally downloads and decrypts the report locally for review.
Step 13: Doctor writes the prescription, encrypts it with AES, and uploads it to IPFS, receiving prescription CID.
Step 14: Invoke uploadPrescription(prescriptionCid) on the smart contract.
IF payment_verified = true
    Store prescription CID on-chain; Status ← Completed
ELSE
    Return Anchor guard error: NotPaid
Step 15: Patient opens the inbox; the system fetches all PDAs linked to the connected wallet only.
Step 16: Patient downloads the encrypted prescription by its CID from the IPFS gateway.
Step 17: Decrypt the prescription locally in the browser and deliver the plaintext file to the patient.
Step 18: Display consultation details, status badges, and all on-chain transaction signatures as Solana explorer links.
Step 19: Continue monitoring for new consultations linked to the wallet.
Step 20: End.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. SIMULATION RESULTS

The proposed Online Anonymous Medical Service System was implemented using Next.js 14 with TypeScript for the frontend, Rust with the Anchor framework (v0.30.1) for the smart contract, crypto-js for browser-side AES encryption, and Pinata for IPFS pinning. The application was deployed live on Vercel with the Anchor program deployed to Solana Devnet, and was exercised through the complete five-step consultation workflow across multiple consultations using a Phantom wallet. All state transitions — consultation creation, payment verification, and prescription completion — were confirmed as immutable on-chain records viewable on the Solana explorer.

In addition to functional validation, the system was evaluated for privacy and fairness properties. No personal data was collected or transmitted at any point during the demonstration: the patient was identified solely by the wallet public key, all documents traversed the network only as AES ciphertexts, and prescriptions were decrypted exclusively inside the patient browser. The Anchor state machine correctly rejected out-of-order operations, enforcing that a prescription can only be uploaded to a consultation whose payment has been verified on-chain, thereby realizing the weak-fairness guarantee. The complete workflow was demonstrable in under three minutes using only a browser and the Phantom wallet extension.

A. Evaluation and Interpretation of System Interfaces:

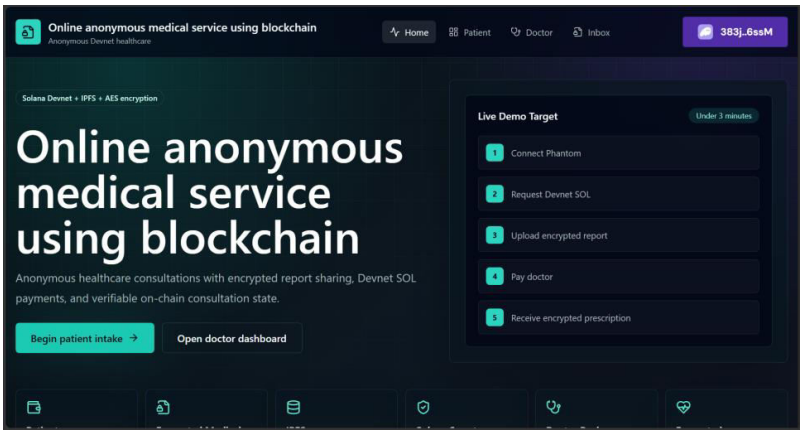


Fig. 2. Home Page – Live Demo Overview

Figure 2 shows the home page with the Phantom wallet connected. The Live Demo Target panel lists the five consultation steps, and the tagline confirms the core privacy property: anonymous healthcare consultations with encrypted report sharing, Devnet SOL payments, and verifiable on-chain consultation state.

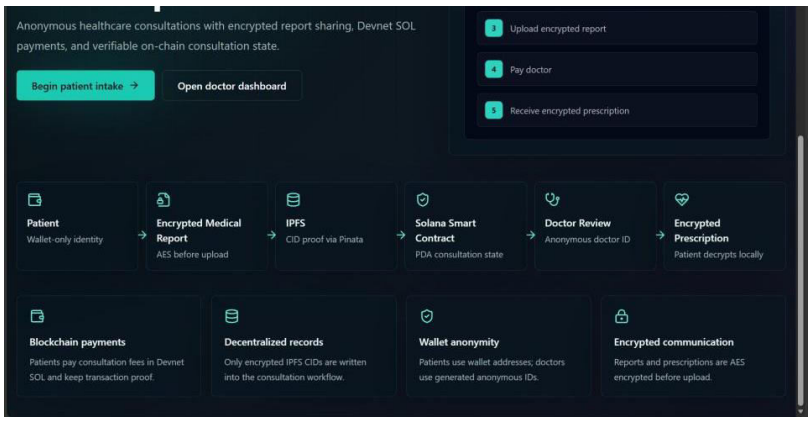


Fig. 3. Patient Dashboard – Wallet and New Consultation

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Figure 3 shows the patient dashboard. The wallet section displays the anonymous alias and Devnet balance with an airdrop button. The new consultation panel orchestrates encryption, IPFS upload, PDA creation, payment, and verification behind a single action button, and completed consultations are listed with encrypted report CIDs and payment transaction links.

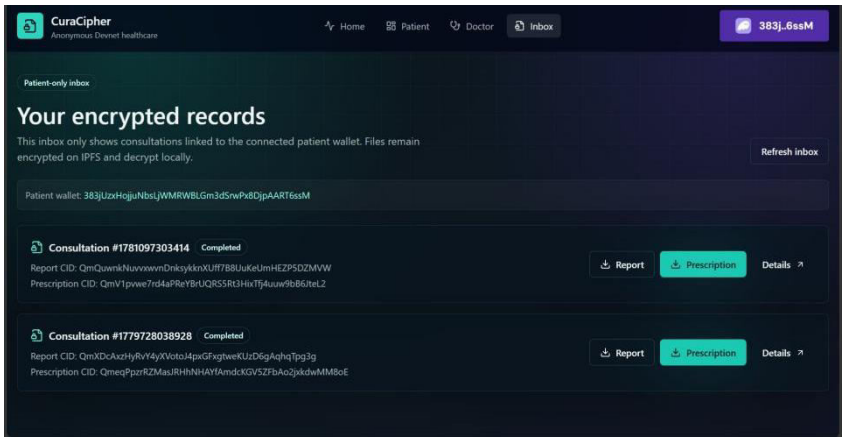


Fig. 4. Phantom Wallet – Confirm Transaction for PDA Creation

Figure 4 shows the Phantom transaction confirmation dialog for consultation PDA creation, displaying the application domain, the estimated account-rent deduction, and the network fee. Transaction signing happens entirely within the Phantom extension, confirming that the private key is never accessible to the application.

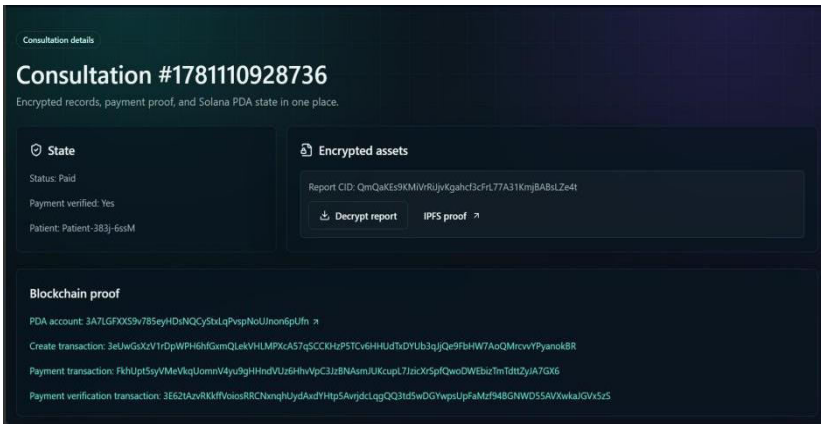


Fig. 5. Consultation Details – Blockchain Proof and Encrypted Assets

Figure 5 shows the consultation detail page. The state panel confirms Status: Paid and Payment verified: Yes. The blockchain proof section lists the PDA account address, the creation transaction signature, the payment transaction signature, and the payment verification transaction as Solana explorer links — demonstrating the complete immutable audit trail with no personal information.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

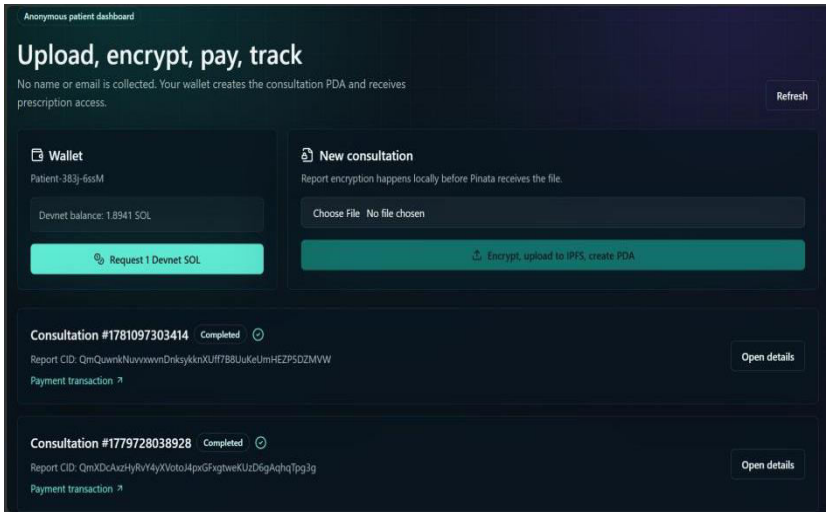


Fig. 6. Patient Inbox – Encrypted Records and Prescription Download

Figure 6 shows the patient inbox. Completed consultations are listed with report and prescription CIDs. Selecting a prescription fetches the encrypted content from IPFS, decrypts it locally in the browser, and triggers a plaintext download — confirming end-to-end privacy.

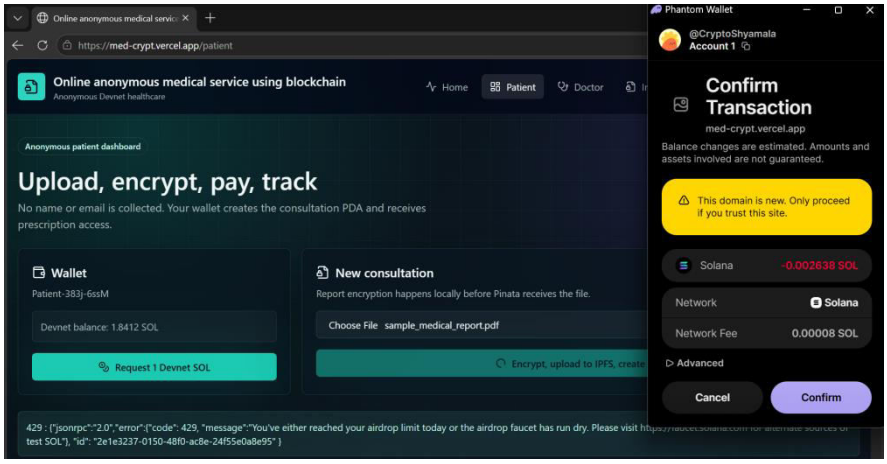


Fig. 7. Doctor Dashboard – Review and Upload Encrypted Prescription

Figure 7 shows the doctor dashboard with a generated anonymous doctor identity derived from the doctor wallet, confirming that no real doctor profile is stored. The paid consultation queue displays verified payment status and encrypted report CIDs, and the secure prescription panel handles encryption, IPFS upload, and on-chain completion.

B. Metrics for Evaluation:

The performance of the proposed system is evaluated through functional, integration, end-to-end, and negative test cases executed against the live Solana Devnet deployment. These tests measure the correctness of the AES encryption round-trip, IPFS content addressing, smart-contract state-machine enforcement, wallet-scoped access control, and the complete anonymous consultation workflow. All test cases passed, as summarized in Table 1.

© 2026 IJIRCCE | Volume 14, Issue 7, July 2026 DOI: 10.15680/IJIRCCE.2026.1407052

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 1. Test Cases and Results

Test Case	Input	Expected Output	Result
AES round-trip (PDF)	Sample PDF file	Decrypted output == original bytes	Pass
IPFS upload	Encrypted blob	Valid CID; content retrievable	Pass
Create PDA	Consultation ID + CID	PDA created; status Created	Pass
Duplicate PDA	Same consultation ID	Anchor error; transaction fails	Pass
Pay and verify	SOL transfer + verifyPayment	PDA status = Paid	Pass
Upload on unpaid	uploadPrescription on Created	Anchor guard error: NotPaid	Pass
Upload prescription	Prescription CID on Paid PDA	Status = Completed; CID stored	Pass
Inbox wallet filter	Different wallet connected	No consultations displayed	Pass
Prescription download	prescriptionCID from inbox	Decrypted file downloads correctly	Pass
Zero balance airdrop	Wallet with 0 SOL	1 Devnet SOL added to balance	Pass

Beyond functional correctness, the evaluation confirms three security properties. Privacy: no personal identifiers exist at any system layer, and all documents traverse the network only as ciphertext. Fairness: the on-chain guard requiring payment verification before prescription upload realizes weak fairness — either both parties receive their deliverable or neither does. Verifiability: every payment and state transition produces a publicly verifiable transaction signature on the Solana explorer, providing non-repudiation without any trusted third party.

VI. CONCLUSION AND FUTURE WORK

This work has demonstrated that a fully functional, end-to-end anonymous online medical consultation system can be realized using publicly available blockchain, decentralized storage, and browser-based encryption technologies. The proposed system achieves what existing telemedicine platforms do not: the structural elimination of personal data from the technical architecture. Patients are identified solely by cryptographic wallet addresses, medical documents are AES-encrypted before leaving the browser, consultation state is recorded immutably on Solana through Anchor Program Derived Accounts, and prescriptions are delivered as encrypted IPFS files decryptable only on the patient device. The fair-exchange framework was successfully adapted from a physical-material service context to an online-only healthcare workflow, with the smart contract enforcing protocol rules in executable code and providing non-repudiation without a trusted third party. Experimental results confirm correct multi-consultation tracking, on-chain payment verification, local decryption of prescriptions, and wallet-scoped access control. Future work will concentrate on replacing the shared demonstration key with patient-controlled public-key encryption for true end-to-end encryption, adding cryptographic authorization of doctor wallets, integrating decentralized dispute resolution (e.g., Kleros) for unresponsive consultations, conducting a formal HIPAA and GDPR compliance review for Solana mainnet deployment, and extending the system to support multi-doctor routing and specialty matching while preserving patient anonymity.

REFERENCES

1. S. Baranski, J. Szymanski, and H. Mora, “Anonymous provision of privacy-sensitive services using blockchain and decentralised storage,” International Journal of Information Security, vol. 24, 130, 2025.
2. R. AlTawy, M. ElSheikh, A. M. Youssef, and G. Gong, “Lelantos: A Blockchain-Based Anonymous Physical Delivery System,” in Proc. 15th Annual Conference on Privacy, Security and Trust (PST), pp. 15–1 to 15–9, 2017.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

3. M. F. Hinarejos, J.-L. Ferrer-Gomila, and L. Huguet-Rotger, "A solution for secure certified electronic mail using blockchain as a secure message board," IEEE Access, vol. 7, pp. 31330–31341, 2019.
4. H. Meng, E. Bian, and C. Tang, "Themis: Towards decentralized escrow of cryptocurrencies without trusted third parties," in Proc. 6th International Conference on Software Defined Systems (SDS), pp. 266–271, 2019.
5. H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," IEEE Access, vol. 7, pp. 61656–61669, 2019.
6. I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," Egyptian Informatics Journal, vol. 22, no. 2, pp. 177–183, 2021.
7. V. S. Naresh and M. Thamarai, "Privacy-preserving data mining and machine learning in healthcare," WIREs Data Mining and Knowledge Discovery, vol. 13, no. 2, e1490, 2023.
8. J. Benet, "IPFS – Content Addressed, Versioned, P2P File System," arXiv:1407.3561, 2014.
9. Protocol Labs, "Filecoin: A Decentralized Storage Network," Technical Whitepaper, 2017.
10. D. J. Solove, "A taxonomy of privacy," University of Pennsylvania Law Review, vol. 154, no. 3, pp. 477–564, 2006.
11. L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557–570, 2002.
12. K. J. Black, S. K. Barton, and J. S. Perlmutter, "Presymptomatic testing and confidentiality in the age of the electronic medical record," Journal of Neuropsychiatry and Clinical Neurosciences, vol. 33, no. 1, pp. 80–83, 2021.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details