IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

# MatdaanX: Decentralised Blockchain and IoT Based Secure Voting System

**H C Pranjali Holla[1], Dr C A Bindyashree [2], Chandhana B C[3], Deekshitha N[4], K Harshini[5]**

Department of Information Science and Engineering, The Oxford College of Engineering,

Affiliated to Visvesvaraya Technological University, Belagavi, Karnataka, India[1-5]

**Abstract**: MatdaanX is a decentralized hybrid voting architecture designed to deliver secure, transparent, and reliable election processes through the integration of blockchain technology, biometrics, and IoT-based offline modules. MatdaanX is a secure and transparent electronic voting platform developed to make the election process more dependable and user friendly. The online module authenticates voters through multiple layers of verification, including facial recognition based on MTCNN, OTP verification, and digital signatures. This ensures that each vote is genuine and securely encrypted before being submitted. In regions with poor or unstable internet connectivity, the system offers an offline setup that operates using an Arduino Uno microcontroller integrated with a fingerprint sensor, keypad, and LCD display. This allows voters to cast their ballots effortlessly without relying on continuous network access, ensuring inclusive participation in all areas. Both online and offline votes in MatdaanX are securely recorded in a private blockchain network that employs SHA-256 hashing along with a Proof- of-Authority(POA) consensus model. This approach guarantees data integrity, transparency, and resistance to any form of tampering or unauthorized modification By integrating biometric verification, blockchain-based recordkeeping, and dual online-offline connectivity, MatdaanX effectively tackles major electoral challenges such as voter fraud, duplicate entries, ballot manipulation, limited accessibility, and delays in result compilation. Overall, it offers a transparent, verifiable, and inclusive framework for conducting elections in a modern democratic environment.

**Keywords:** Blockchain, Biometric Authentication, IoT, Secure E-Voting, Face Recognition, Fingerprint Scanning, Decentralized Systems.

## I. INTRODUCTION

Modern electoral systems still encounter significant challenges in maintaining security, protecting voter privacy, ensuring transparency, and achieving scalability and accessibility for all citizens. Traditional methods such as paper ballots and electronic voting machines (EVMs) often lack advanced mechanisms for verifying voter identity, detecting tampering, and enabling reliable audit trials. This study introduces MatdaanX, a blockchain-Enabled Hybrid Voting Framework that integrates both online and offline voting methods into a unified, secure, and transparent platform. Built into MatdaanX, safeguards ensure votes stay protected while still easy to reach. Protection and access walk hand in hand here, shaped quietly behind the scenes. With online voting, face scans helped confirm identity. The system used MTCNN to detect faces accurately. Authentication happened by matching live images to stored data. This method aimed to reduce false access attempts. Each check focused on key facial landmarks. Security improved through precise alignment steps. Verification occurred before allowing ballot submission Who the person voting is. A quick code arrives by message, meant for just you. This extra step helps confirm it is really you trying to log in. Votes get a digital signature once the voter is confirmed, then saved on a blockchain system. The moment identity checks out, encryption locks the ballot in place across distributed nodes. Nothing can change the vote once this is done. Folks pointed out how hard it is to get steady internet where roads turn to dirt. Out there, far from cities, signals often fade before they arrive. Here's how it works in MatdaanX - built around a hands-on voting tool made with an Arduino Uno, crafted step by step without relying on online access a Fingerprint device. A small keypad sits there too. People living far from cities can vote even when internet connections are weak or unreliable because this system works without needing constant online access. Some choose fast options, others look for safety first. Trust matters when picking one over another. Once connected again, voting data flows into the database - every bit accounted for without exception. Not a single vote will disappear or change while things are happening. By checking who you are, locking information away tight, then moving it to spots where nothing gets wiped - the setup wipes out the issues associated with a single point of control. Voting more than one time isn't allowed for any person. Each individual gets just a single choice. When elections happen, your vote stays private. Security measures protect it completely. Officials who need to check things can look - only if allowed. Because these setups include internet-based and paper ballots, access spreads more evenly across different groups. One reason is that not everyone connects the same way. Some rely on devices, others prefer physical forms. Mixing methods opens paths where one might close.

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

## II. PROBLEM STATEMENT AND OBJECTIVE

### A. Existing System Vulnerabilities

Traditional centralized voting systems face significant vulnerabilities. When voter information and ballots are stored in a single centralized database, it creates multiple points of weak- ness exploitable for unauthorized access, ballot tampering, or large-scale result manipulation.

These conventional systems often lack strong mechanisms for voter authentication, prevention of duplicate voting, and end-to-end transparency. In regions with poor network infrastructure, the absence of secure digital identity verification and reliable vote recording further limits participation.

### B. Objectives

The MatdaanX framework addresses these issues through:

- Ensuring robust voter authentication through biometric verification
- Providing transparent and tamper-proof vote storage using blockchain
- Applying cryptographic protocols to prevent duplicate voting and identity fraud
- Promoting inclusive elections through hybrid online and offline voting
- Enhancing security, scalability, and reliability across different environments.

## III. SCOPE

We've attempted with MatdaanX to address what we see as the most pressing issues in present day voting systems. We are using biometric authentication for voter identification and secure record of their votes which in turn reduces the issues that come with centralized databases and manual verification. This approach we put forth builds that trust between the voter and the system, protects the integrity of the election data and also brings in an element of transparency which permeates the entire voting process. At the base of MatdaanX we have blockchain technology.

Once a vote has been cast it is permanent and out of question for alteration or removal. Every vote leaves a trace which authorized officials may audit. Security is a multilayer approach which we see in many forms, they work together. Biometric verification is used at many stages, also we have protection of the votes. We have a number of items that are put in place to secure and also continuous improvements are made to the systems. As a result we see better at identifying and putting a stop to unauthorized activity and also we identify and address gaps that were not before. And also it is a fact that MatdaanX has a dual mode design which is one of its greatest assets. In urban areas which have reliable internet we see online voting and in outlying areas we have offline hardware modules. This means that poor connectivity can never serve as a reason to block people from voting. Given that the system is decentralized, it can scale efficiently and accommodate many voters in different regions without crashing. MatdaanX is also pragmatically designed. It can function with unreliable power, poor internet, and minimal user.

## IV. LITERATURE REVIEW

Several approaches have been proposed for e-voting systems.

[1] Gupta et al. developed a blockchain e-voting protocol recording encrypted ballots on distributed ledgers, though relying on password authentication making it susceptible to phishing.

[2] Sharma et al. introduced OTP-based two-factor verification, but maintained centralized vote databases creating single points of failure.

[3] Patel et al. enhanced EVMs with fingerprint authentication, preventing impersonation but lacking comprehensive end-to-end verifiability.

[4] Lee et al. designed smart contract- based voting on public blockchains, assuming constant internet availability and overlooking offline scenarios.

[5] Santos et al. combined homomorphic encryption with blockchain, boosting privacy but creating impractical computational requirements for low-resource devices.

[6] Kim et al. explored permissioned blockchains using trusted node consortia, reducing energy consumption but lacking biometric safeguards.

[7] Rossi et al. created IoT-based voting with embedded devices, improving usability but lacking blockchain integration.

[8] Al-Hashimi et al. implemented deep learning face recognition, achieving high accuracy but remaining vulnerable to backend manipulation.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

A. *Research Gaps*

While progress has been made, several challenges persist. Most blockchain voting systems lack integrated hybrid architectures supporting both online and offline participation. Multi layered biometric verification systems with cryptographic linking are rarely applied. Scalability remains significant, with public blockchains experiencing transaction delays and congestion.

The absence of affordable IoT-based voting devices for offline use restricts large-scale deployment. Computational efficiency remains pressing, as cryptographic algorithms and biometric processing place heavy demands on low-power devices.

## V. SYSTEM ARCHITECTURE

MatdaanX combines a secure web-based online voting platform with dedicated IoT offline hardware, both integrated with a private blockchain. The system architecture is depicted in Fig. 1.

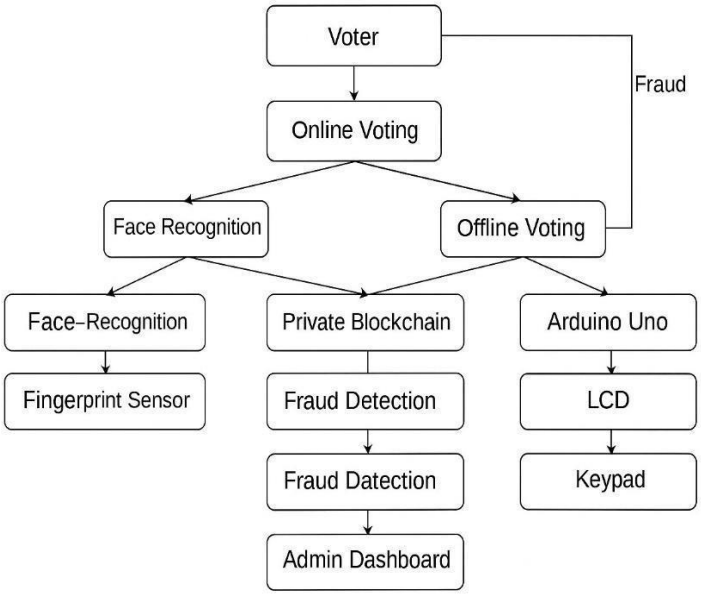


Fig. 1. Complete system architecture showing integration of online and offline voting, biometric authentication, private blockchain validation, fraud detection, and admin dashboard

A. Online Module

The Flask-powered web interface serves as the gateway for online participation, handling facial recognition via MTCNN, OTP validation, and blockchain interactions. Voter identity undergoes dual verification, checks for prior voting activity, followed by cryptographic signing and encryption before submission as a blockchain transaction.

B. Offline Module

The offline module offers an alternative built around Arduino Uno integrated with fingerprint scanner, numeric keypad, LCD screen, and audio feedback. Local fingerprint authentication confirms voter identity while keypad input captures candidate selection. Encrypted votes with timestamps remain stored on device until network restoration enables synchronization to the private blockchain.

C. Blockchain Integration

Every ballot cast is securely stored as a unique blockchain transaction. Each block is encrypted using SHA-256 hashing algorithm, while a Proof-of-Authority (PoA) consensus mechanism enables fast validation through preauthorized election nodes.

Smart contracts automate essential election functions such as verifying voter IDs to prevent duplicate voting, validating ballot submissions, and managing secure access to tallying operations.

## VI. METHODOLOGY

A. *Voter Enrollment and Biometric Registration*

During registration, election authorities securely collect voter information including voter ID, demographic details, and

  

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.1412137

biometric data. Online voters provide high-resolution facial images processed into embedding vectors via MTCNN. Offline participants register fingerprint templates through IoT-based voting terminals.

B. *Online Authentication and Vote Preparation*

The online pathway implements multi-factor authentication:

1) MTCNN facial recognition compares live captures against stored embeddings
2) OTP delivery validates registered contacts
3) Cryptographic device signatures bind voter identity to the ballot

Only after completing all verification steps does the system encrypt the vote for blockchain submission.

C. *Offline IoT Voting Protocol*

For connectivity-challenged areas, MatdaanX deploys Arduino Uno-based voting stations equipped with:

- Fingerprint sensors for voter identity confirmation
- Keypads for intuitive candidate selection
- LCD displays for navigational guidance
- Local encryption for timestamp and metadata security Encrypted ballots remain stored on-device until network

restoration triggers blockchain synchronization

TABLE I
VOTE TRANSACTION STRUCTURE

| Field | Description |
|---|---|
| Voter Hash | SHA-256 hash of biometric-derived ID |
| Candidate ID | Encoded selection choice |
| Timestamp | Vote casting time |
| Mode | Online / Offline |
| Encrypted Payload | AES-encrypted vote packet |
| Digital Signature | ECDSA signature for authenticity |

TABLE II
SAMPLE OFFLINE VOTE LOG STRUCTURE

| Timestamp | Station | FP ID | Candidate | Status |
|---|---|---|---|---|
| 09:45 | PS-14 | FP 3021 | CND 02 | Stored |
| 09:50 | PS-14 | FP 1077 | CND 01 | Stored |
| 10:03 | PS-14 | FP 3021 | CND 03 | Synced |

D. *Biometric Verification and Vote Packaging*

Post verification, each ballot assembles a comprehensive data package containing:

- Pseudonymized voter identifier
- Selected candidate identifier
- Precise timestamp
- Voting modality (online/offline)
- Device cryptographic signature

The structure undergoes AES encryption followed by ECDSA digital signing.

E. *Blockchain-Based Validation*

All voting transactions are validated through a private blockchain using PoA consensus:

1) Blockchain nodes verify digital transaction signatures
2) System checks for duplicate timestamps and voter IDs
3) Valid transactions are grouped into blocks
4) Each block undergoes SHA-256 hashing
5) Finalized block is appended to blockchain ledger

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

F. *Offline Vote Synchronization*

IoT-based voting devices securely store encrypted votes locally when network connectivity is unavailable. Upon connectivity restoration:

1) Device sends batch upload request to gateway server
2) Encrypted ballots are transmitted securely
3) System performs duplicate fingerprint and voter hash checks
4) After verification, approved votes are committed to blockchain

G. *Fraud Detection Engine*

The system includes real-time fraud detection monitoring both channels for anomalies:

- Multiple OTP requests
- Repeated facial recognition failures
- Duplicate biometric matches
- Automated voting patterns
- Irregular node behavior
- When threats are detected, the system immediately suspends sessions, flags polling stations, or places suspicious transactions on hold

## VII. IMPLEMENATION ENVIRONMENT

Python forms the backbone of core security operations including MTCNN-based facial recognition, fingerprint template matching, AES encryption, SHA-256 hashing, ECDSA digital signing, OTP verification, and offline synchronization. Solidity develops smart contracts managing vote recording, duplicate prevention, validator authorization, and result tallying. These contracts ensure transparent and immutable transaction processing. Ganache provides a simulated local Ethereum test network for development and testing, enabling deployment of smart contracts and validation of PoA consensus without real gas fees.Web3.py acts as bridge between Python backend and blockchain network, handling encrypted vote submissions, smart contract interactions, and immutable vote logging through JSON-RPC communication. Flask powers the web voting portal and administrative dash- board, managing user sessions, biometric authentication, OTP generation, encryption routines, and blockchain API requests.SHA-256 generates fixed 256-bit hash values demonstrating collision resistance where minimal input changes produce entirely different outputs. Processing 512-bit chunks through 64 computational rounds ensures complete tamper-proofing.


Figure 3: Dashboard of Online voting system

The Arduino Uno, built around the ATmega328P microcontroller, operates at 5V with comprehensive digital and analog I/O pins. It seamlessly connects to biometric sensors, keypads, and displays, ensuring reliable real-time performance in network-independent scenarios. MatdaanX integrates a dedicated fingerprint sensor powered at 3.3V-5V, capturing high-resolution images and converting them to digital templates. The onboard processor performs local matching, reducing Arduino computational demands.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

Algorithm SHA256_Hash(M) Input: Message M
Output: 256-bit HashValue 1: M ← PadMessage(M)
2: Blocks ← SplitInto512Bit 3: Initialize hash values H0.H7 4: for Block in Blocks:
5: W ← MessageSchedule(Block) 6: a, b, c, d, e, f, g, h <- H0.H7
7: for i = 0 to
end
8: T1 ← h + ∑1(e) + Ch(e, f, g) + K[i] + W[i]
9: T2 = Σ2(a) + M aj(a,b,c)
10: h = g; g = f; f = e 11: e ← d + T1
12: d = c; c = b; b = a 13: a <- T1 + T2
14: end for
15: H0.H7 <- (a.h)
16: end for

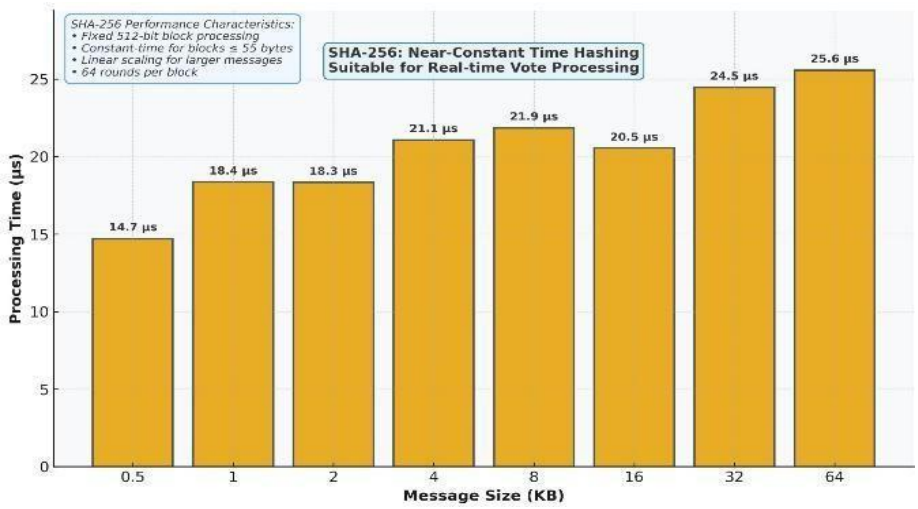


Figure 4: SHA-256 Hashing Performance Analysis

The numerical keypad plays a crucial role in helping voters select their preferred candidates when voting offline. It works reliably across a voltage range of 3.3V to 5V and doesn't require complicated wiring, making it perfect for portable voting terminals that need to be set up quickly in different locations. The keys provide satisfying tactile feedback when pressed, and the keypad itself is built tough enough to withstand regular handling in various field conditions whether that's a dusty village hall or a makeshift polling booth under a tent. The LCD screen acts as the voter's guide throughout the entire process. Once upon a vote being cast it is made permanent and does not see change or removal. Each vote leaves a which is clear and traceable for authorized officials to audit.

Security is not in a single method, many layers of security which work together. Biometric verification is used at many stages, we protect the votes. We put in safeguards for individual items and also see to it that we are constantly improving the systems. As a result we are better at identifying and stopping unauthorized system activity also we are more at to notice and report unaddressed gaps. And in that which we present to you MatdaanX we see one of its great assets in its dual mode design. In urban areas which have stable internet we see that voting online is an option, for the outlying areas we have the offline solution hardware modules. Inequity in cell and internet coverage should not hinder individuals from exercising their right to participate in an election and vote. Especially when the box displays made for this equipment can easily fit in the user's pocket.

It can display 16 characters per line in two lines, and makes the voting process accessible and easy. It shows users step-by-step instructions from logging in and verifying their identity to arriving at the ballot screen, and from confirming their selection to the final submission. The devices are easy to configure since it only contains four wire connections to the Arduino. The box displays run on 5 volts and include a built in contrast adjustment knob on the back. This knob is for the election workers to adjust in order to make the text clear and readable for each voter, at any time of the day. Even though the tiny buzzer is a small component, it contributes to a more inclusive design system. There is an audio cue for each action taken during the voting process. Users hear a tone when the system successfully authenticates a fingerprint, and a different tone is played when an invalid fingerprint is entered.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

The system plays a tone to acknowledge the registration of the vote. The system plays a confirmation tone when the voting process is completed. Blind users do not have to see the computer screen to vote as the complete the process by audio. The system continues to utilize two additional storage solutions so that no vote is ever lost, even offline. Inside MatdaanX, quiet layers guard every vote without locking it away. Easy reach stays possible because safety works unseen. Balance comes naturally when both sides grow from the same design. Now imagine a camera checking who you are when casting votes online. A tool called MTCNN made sure it saw real faces clearly. Instead of guessing, the setup compared what it captured right then to files already saved. It tried cutting down cases where someone else sneaks in. Attention went straight to specific points on each person's face.

Moves lined up just right, making things safer. Before any vote went in, checks happened first. A message pops up with a short code - only for your eyes. Since it shows up when you sign in, someone else can't easily pretend to be you. A fresh digital mark seals each vote after the person is verified. Once who they are clicks into place, scrambled code tucks the ballot safely inside many linked computers at once. A single vote at a time shapes what happens next in MatdaanX - this system runs on an Arduino Uno, shaped slowly, piece by piece. Step one follows another, each done offline, no internet needed. The core is physical, interactive, tied directly to actions taken nearby.

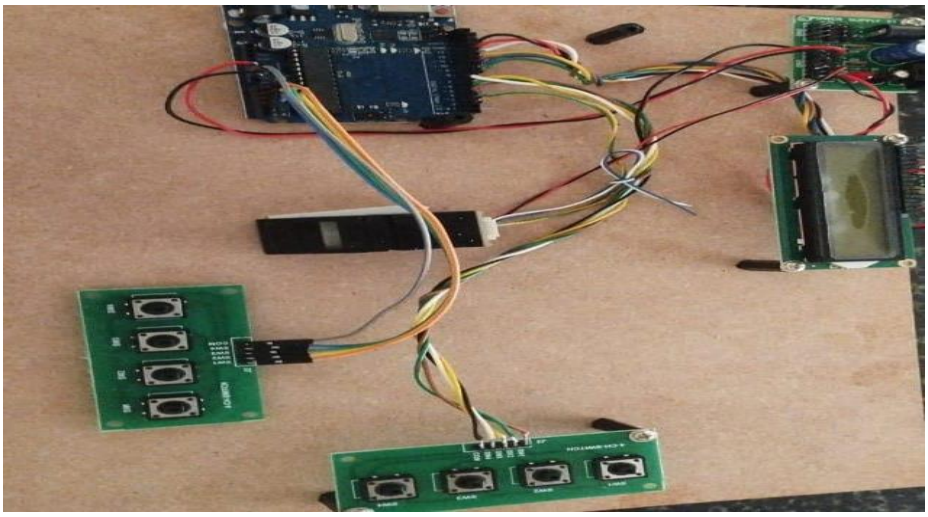

Figure 5: Hardware prototype showing Ardunio based MatdaanX voting unit integrating fingerprint sensor, keypads and LCD interface.

## VIII. MODULES

### 8.1 Online Voting and Biometric Authentication

This part of the system lets people vote securely through a website we built with Flask. It uses facial recognition, sends one-time passwords to your phone, and encrypts your ballot before adding it to the blockchain. The facial recognition technology (MTCNN) works in three stages - it first spots your face, then draws a box around it precisely, and finally identifies specific features like your eyes and nose. This method is both accurate and fast enough to verify voters on the spot. When you submit your photo, the system creates a unique 128-number fingerprint of your face and compares it against the photo you registered with earlier. It measures how similar they are, and if the match is strong enough, you're authenticated and can proceed to vote.

### 8.2 Offline IoT Voting Module

We designed this for rural areas or places where internet is unreliable. It is a stand alone system which we have put together using an Arduino microcontroller, a fingerprint scanner, a keypad, and a small scale display. The fingerprint scanner is used for identification of the voter, also the display which walks the voter through each step. Step by step we have made the voting process easy and friendly for the users. This module also includes voter registration, vote casting, and secure local storage of votes. At registration time we store the voter's fingerprint as a digital template in the Arduino's non-volatile memory.

Which includes key ridge patterns and distinct points. When a voter places their finger on the scanner during the vote the system compares the live fingerprint of the voter against that which is stored in the database. The stored template which is done by matching feature points. If we have a valid match the voter is authenticated and their encrypted vote is recorded secure. You're verified when enough points match which is usually at the 40 to 50 mark for feature match.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.1412137

Since it runs all on the Arduino which doesn't require the internet for it's function voting may go on even during long power cuts or network failures. Each vote is put through AES-128 encryption and we also attach a time stamp and a device ID to it. This allows for the votes to be traced at a later date for verification or audit purposes which at the same time does not reveal any of the voter info. 83 Vote Synchronization and Blockchain Integration Once the internet connection is back the votes which were stored on offline devices' data is uploaded to the blockchain.

### 8.3 Vote Synchronization and Blockchain Integration

Once internet comes back online, votes stored on the offline devices get uploaded securely to the blockchain. Our Web3.py software checks each encrypted vote package, looks for any duplicates, and adds legitimate votes to the permanent record. We built in safeguards so votes don't get lost if the upload gets interrupted. Multiple votes are bundled together to save bandwidth and reduce traffic on the blockchain network. The system is checking out for duplicate votes to make sure that no single vote is counted more than once. Also we have put in a number of safety features to prevent data loss with issue of unstable connections. We upload votes in batches to also reduce network traffic and to put the transaction costs down. In the event of an upload which is interrupted we do not delete the data.

### 8.4 Blockchain Smart Contracts

We wrote smart contracts in Solidity that handle recording votes, blocking duplicates, authorizing officials, and controlling who can view results. These contracts ensure everything stays transparent and can't be tampered with. Different people have different access levels - election commissioners, regional coordinators, and independent auditors each have specific permissions.

The main functions are:

- registerVoter(): Adds new voters with their biometric information
- castVote(): Saves encrypted ballots with digital signatures
- preventDuplicate(): Checks if someone already voted
- getTallyResults(): Shows vote counts to authorized personnel
- auditTrail(): Displays the complete voting record with timestamps

We optimized the contracts to keep transaction fees low by using smart data storage and cutting out wasteful operations. The system broadcasts updates about what's happening on the blockchain so monitoring dashboards can show live information without having to constantly check for changes.

### 8.5 Fraud Detection and Anomaly Monitoring

This component continuously monitors both channels identifying anomalies including excessive OTP requests, facial recognition mismatches, duplicate biometric entries, and ab- normal submission rates. The detection engine employs machine learning-based anomaly detection models trained on historical election data, establishing baseline voting patterns and identifying deviations exceeding statistical thresholds.

Detection rules include:

- Threshold-based alerts: More than 3 failed authentications within 5 minutes triggers account lockout
- Statistical anomalies: Submission rates exceeding mean by more than 3 standard deviations flag polling stations
- Pattern analysis: Identical keyboard entry sequences or facial recognition failures from same terminal indicate attack attempts
- Temporal anomalies: Unusual voting times or geographic inconsistencies suggest compromised devices
- Blockchain anomalies: Irregular transaction patterns, un- usual validator node behavior, or block propagation delays

The fraud engine integrates with incident response systems, automatically suspending suspicious accounts while preserving evidence for forensic analysis.

### 8.6 Administrative Dashboard

The web-based dashboard provides real-time visibility into election operations, displaying total votes, voter turnout, online or offline participation rates, synchronization progress, and fraud alerts. Interactive visualizations employ data aggregation techniques, computing statistics across distributed polling stations without exposing individual voter information.

Dashboard components include:

- Live vote counter: Real-time ballot count with online/of- fline split percentages
- Synchronization monitor: Progress tracking for offline device synchronization queues
- Fraud alert panel: Categorized alerts with severity indicators and remediation recommendations
- Validator performance metrics: Blockchain node responsiveness and consensus participation rates
- Voter turnout trends: Time-series analysis showing participation patterns throughout election day

  

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

- Candidate performance: Vote distribution visualization across candidates (before final tally)
- System health metrics: Server load, bandwidth utilization, database performance indicators

Role-based access control restricts dashboard visibility to authorized personnel, with audit logs tracking all administrative actions for security compliance verification.

## IX. PERFORMANCE EVALUATION

### 9.1 Blockchain Transaction Validation Performance

Blockchain layer responsiveness was assessed by measuring time taken to validate and commit encrypted vote transactions. As shown in Fig. 3, validation completed between 650 ms and 900 ms with consistent sub-second performance confirming suitability for high-volume election environments.

Key observations:

- Iteration 1: Minimal latency (~650 ms) with low initial network load
- Iterations 2-3: Moderate increase (~900 ms) from elevated transaction volume

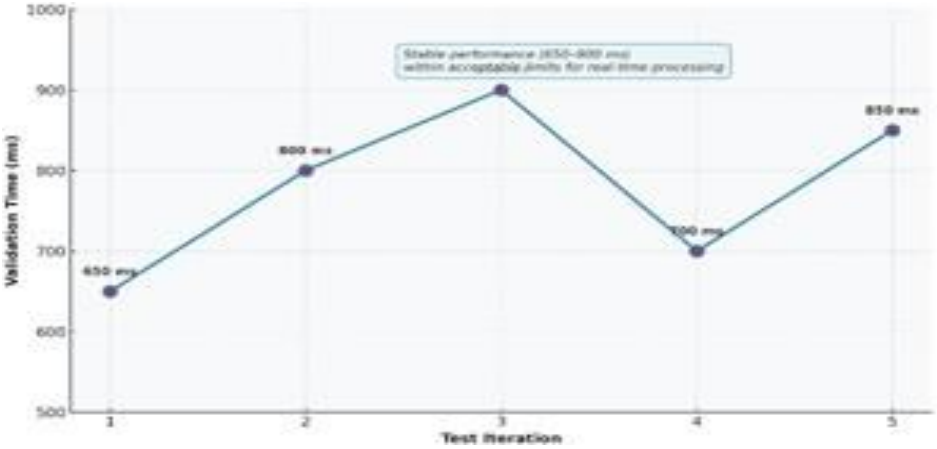


Figure 5: Blockchain Validation Time Across Test Iterations

TABLE III
END-TO-END SYSTEM LATENCY BREAKDOWN

| Process Component | Duration (ms) |
|---|---|
| Biometric Authentication | 200–300 |
| Encryption and Signing | <100 |
| Online Submission | 600–900 |
| Offline Synchronization | 800–1200 |
| Dashboard Updates | 100–200 |
| **Total Latency** | **1500–2400** |

- Iteration 4: Recovered efficiency (~700 ms) as network stabilized
- Iteration 5: Sustained reliable performance (~850 ms) under sustained load

### 9.2 End-to-End Latency Analysis

Complete voting workflow latency was measured across pipeline stages. Table III illustrates timing distribution. Blockchain validation represents the primary latency contributor in decentralized systems, yet all components maintain real-time performance suitable for voter and administrator interactions.

## X. CONCLUSION

MatdaanX represents a comprehensive solution to the critical challenges facing modern elections - security vulnerabilities, transparency gaps, and eroding public trust in voting systems. Instead what we do is we monitor

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.1412137

pending votes and get back to uploading when the system re gains internet connection. As the system is syncing we go through the blockchain record for duplicate entries. If we find duplicates the system will flag them, log them and put the submission in for review. For the purposes of that review system admins are notified. At the same time devices which are casting votes and the server are in constant communication to see that each vote is transmitted and logged successfully. If the system is unable to transmit the vote it will enter a delay and increase the between which we have intervals of vote transmission during which no success is achieved, also in terms of election security which reports large scale security breaches of present voting systems.

Transparency problems which also see trust between the people and the government break down.Out of which the issue of centralized servers which are a single point of failure and isolated electronic machines which are easy targets for hacking we have addressed with the help of our solution MatdaanX which we have designed on the base of blockchain tech and multilayer biometric verification. This we have done to preserve the privacy of the vote at the same time make the process open to verification and permanent. We have designed the system from the voter registration right through to the final count to be very clear and traceable. Also in our system once a vote is cast it cannot be changed, we block any unauthorized changes and thus we are able to secure the integrity of the election at every stage. By means of security, scalability and transparency MatdaanX is put in to play which it does very well even at the scale of large scale elections which may have millions of voters at the same time. We see that admin of the elections are given real time access via intuitive dashboards which in turn display vote action, blockchain confirmation report, system health and also alert on fraud. This live info in hand allows officials to react fast and to make informed decisions all through the election day which in turn sees issues addressed early before they grow into bigger problems.

Future development focuses on several transformative enhancements that will further strengthen the platform's capabilities. Adaptive authentication mechanisms will intelligently select verification methods - facial recognition, fingerprint scanning, voice biometrics, or combinations thereof - based on contextual risk assessment, user behavior patterns, and device trustworthiness to minimize impersonation risks. The blockchain infrastructure will transition toward consortium governance models where validation authority is distributed across multiple independent entities rather than concentrated in single organizations, creating more balanced trust distribution. Consensus mechanisms will incorporate advanced protocols including Proof of Authority variants, Byzantine Fault Tolerance algorithms, or hybrid approaches designed to reduce transaction latency and increase processing throughput during peak voting loads. Zero-knowledge proof technology will enable the system to verify voter eligibility and ballot validity without exposing voter identities, while incentive-based smart contracts will ensure validator reliability even under high-demand conditions.

The roadmap ahead includes artificial intelligence systems that predict and prevent fraudulent activities through pattern recognition before violations occur, dynamically calibrated biometric verification that adjusts sensitivity thresholds based on real-time threat assessments, optimized consensus algorithms capable of processing massive transaction volumes, secure metadata indexing enabling comprehensive audits while preserving voter privacy, collaborative frameworks involving multiple independent election oversight authorities, and edge computing capabilities that autonomously detect and respond to security threats at their source. These technological advancements will collectively position MatdaanX as a voting platform secure enough for national elections, scalable enough for the world's largest democracies, accessible enough for the most isolated communities, and resilient enough to withstand both current and emerging threats. Whether citizens vote from urban centers with robust infrastructure or remote villages with limited connectivity, MatdaanX delivers consistent security, reliability, and trustworthiness that strengthens democratic participation and restores public confidence in electoral processes.

## ACKNOWLEDGMENT

The authors thank the faculty and staff of the Department of Information Science and Engineering at The Oxford College of Engineering for their advice and assistance. We are grateful to the open-source communities that support Web3, IPFS, and Ganache as well as to **Dr C. A. Bindyashree** for her technical advice and mentoring.

## REFERENCES

[1]. R. Alami, A. Biswas, V. Shinde, A. Almogren, A. U. Rehman, and T. Shaikh, "Blockchain enabled federated learning for detection of malicious Internet of Things nodes," IEEE Access, 2024
[2]. S. H. Alsamhi, R. Myrzashova, A. Hawbani, S. Kumar, S. Srivastava, L. Zhao, X. Wei, M. Guizan, and E. Curry, "Federated learning meets blockchain in decentralized data-sharing: Healthcare use case," IEEE Internet of Things Journal, 2024

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412137

[3]. C. Ying, F. Xia, D. S. L. Wei, X. Yu, Y. Xu, W. Zhang, X. Jiang, et al., "BIT-FL: Blockchain-enabled incentivized and secure federated learning framework," IEEE Transactions on Mobile Computing, 2024

[4]. S. Yuan, B. Cao, Y. Sun, Z. Wan, and M. Peng, "Secure and efficient federated learning through layering and sharding blockchain," IEEE Transactions on Network Science and Engineering, vol. 11, no. 3, pp. 3120–3134, 2024

[5]. R. Lin, F. Wang, S. Luo, X. Wang, and M. Zukerman, "Time-efficient blockchain-based federated learning,"IEEE/ACM Transactions on Networking, 2024

[6]. H. Huang, L. Duan, C. Li, and W. Ni, "A secure and lightweight aggregation method for blockchain-based distributed federated learning," in Proc. 2024 IEEE Int. Conf. Web Services (ICWS), pp. 447–456, IEEE, 2024

[7]. S. T. Ahmed, T. R. Mahesh, E. Srividhya, V. Vinoth Kumar, S. B. Khan, A. Albuali, and A. Almusharraf, "Towards blockchain-based federated learning in categorizing healthcare monitoring devices on artificial intelligence of medical things investigative framework," BMC Medical Imaging, vol. 24, no. 1, p. 105, 2024

[8]. N. Dong, Z. Wang, J. Sun, M. Kampffmeyer, W. Knottenbelt, and E. Xing, "Defending against poisoning attacks in federated learning with blockchain," IEEE Transactions on Artificial Intelligence, 2024

[9]. X. Yang and C. Xing, "Federated medical learning framework based on blockchain and homomorphic encryption," Wireless Communications and Mobile Computing, vol. 2024, no. 1, Article ID 8138644, 2024

[10]. W. Issa, N. Moustafa, B. Turnbull, N. Sohrabi, and Z. Tari, "Blockchain-based federated learning for securing Internet of Things: A comprehensive survey," ACM Computing Surveys, vol. 55, no. 9, pp. 1–43, 2023

  