AI-IoT Based Smart Election Authentication and Integrity Monitoring System

1.Prof. S. N. Wangikar, 2.Kalyani V. Gurav, 3.Saniya F. Mujawar, 4.Dyaneshwari A. Waghmare

Project guide, Student member, Student member, Student member of

DR.ASHOK GUJAR TECHNICAL INSTITUTE'S

DR.DAULTRAO AHER COLLEGE OF ENGINEERING, KARAD

Department of Electronics and Telecommunication Engineering

Shivaji University,Kolhapur

Abstract -Conventional polling relies on manual identity checks, isolated voting machines and paper-based reporting, which leave room for impersonation, double voting, booth tampering and slow counting. This paper presents the design of SecureVoteGuard, an AI-IoT based smart election authentication and integrity monitoring system built around a low-cost ESP32 controller. A voter is verified in three successive stages: an RFID card read by an RC522 module, face matching on an ESP32 camera image, and fingerprint matching on a DY50 optical sensor. The candidate buttons are unlocked only when all three stages pass. A duplicate-vote check against a cloud database marks each voter as "Voted" the moment a vote is cast, tamper switches in the enclosure raise local alarms and cloud alerts when the unit is opened, and a real-time dashboard shows voter verification, votes cast, authentication failures and tampering alerts to the election officer. The prototype is planned as a mini polling booth and is expected to provide three-layer authentication, instant duplicate-vote rejection, immediate tamper alerts and live monitoring at an estimated cost of about Rs. 7000.

Key Words: Smart Election, Electronic Voting, Artificial Intelligence, Internet of Things, RFID, Face Recognition, Fingerprint, ESP32.

1. INTRODUCTION

Democracy depends on every eligible citizen voting once, and on everyone being able to trust that each recorded vote is genuine. In many polling stations, however, the voter is still identified by a glance at an ID card, standalone machines cannot tell whether the same person has voted elsewhere, and trouble at a booth may reach the election headquarters only after hours. These weaknesses make impersonation, double voting and booth capturing hard to detect and slow to correct.

Several technologies are now cheap and mature enough to address them. RFID gives every voter card a machine-readable identity, face recognition and fingerprint sensors add biometric checks that a stolen card cannot satisfy, low-power microcontrollers with built-in Wi-Fi connect each booth to the cloud, and simple switches can sense physical interference. Used together they allow a booth that verifies voters in layers, refuses a second vote, reports tampering as it happens and lets officers watch the process live.

In this paper we present SecureVoteGuard, a smart election authentication and integrity monitoring system built around one ESP32 controller. Section 2 surveys earlier work, Section 3 identifies the shortcomings of present practice, Section 4 sets out our objectives and scope, Section 5 describes the architecture and its working, Section 6 lists the hardware and method, and Section 7 concludes with the expected outcomes.

2. LITERATURE REVIEW

Earlier research on electronic voting concentrated mainly on fingerprint-based voter identification. A fingerprint alone can fail because of environmental and physical conditions such as dirt, moisture or worn skin, so recent studies recommend combining several methods, such as RFID, face recognition and fingerprint, to improve voter security [1]-[5].

Manoj et al. [1] proposed a secured biometric voting system that authenticates voters through fingerprint, facial recognition, RFID and Aadhaar integration and so prevents duplicate voting. Other work combines IoT devices with fingerprint, face, iris and QR-based verification, and applies biometric template protection to preserve privacy and prevent voter impersonation.

A dual-authentication voting system [2] uses CNN-based facial recognition followed by fingerprint verification, giving two-step authentication, and securely records a single vote on a cloud server. Cloud-enabled biometric authentication has been used to strengthen voter identity verification [3], and a fingerprint-authenticated system with an Android application shares voting data in real time [4]. A hybrid electronic voting system integrating fingerprint and face recognition is described in [5].

Most of these systems concentrate on identifying the voter. The present work instead places three-layer authentication, duplicate-vote checking, physical tamper detection, local and remote alerts and a live officer dashboard on a single inexpensive ESP32 controller.

3. PROBLEM IDENTIFICATION

Present polling arrangements suffer from a set of linked problems. Outdated manual identity verification lets fraudulent voters pass with fake or stolen ID cards. Offline, standalone

voting machines cannot track whether a person votes at more than one location, so double voting goes unnoticed.

Standard voting units have no built-in sensors to detect that the box is being broken open or interfered with, which makes booth capturing hard to detect. The central election headquarters cannot see security breaches or machine failures as they occur, and manual record checking and physical transport of data cause long delays in counting.

4. OBJECTIVES AND SCOPE

The main aim is to build an automated, secure and transparent election booth that verifies every voter, allows one vote per person and reports threats to the officers in real time. In particular, the work sets out to:

(i) authenticate identity in three layers: RFID card, face match and fingerprint; (ii) prevent duplicate voting by checking and updating the voter's status in a cloud database; (iii) monitor the integrity of the voting unit with tamper switches and raise automatic local and remote alerts; and (iv) provide a real-time dashboard and mobile application for remote management by election officers, then test the assembled prototype with valid, duplicate and fake voters.

The design targets a mini polling booth prototype in which voter cards, photographs and fingerprints are pre-registered in a secure cloud database. Candidate push-buttons are enabled only after all three identity stages pass, and the voter's status changes to "Voted" the moment a button is pressed. Later versions could extend the design to multiple booths and add analytics on turnout and security events.

5. PROPOSED SYSTEM

The architecture is centred on an ESP32 microcontroller, which gathers sensor inputs, runs the verification sequence, drives the outputs and communicates over Wi-Fi. Input devices (RC522 RFID module, ESP32 camera, DY50 optical fingerprint sensor and candidate push-buttons) feed the controller, which exchanges data with the database and the remote IoT cloud and drives the local alerts. The overall arrangement is given in Fig -1.

5.1 Three-layer voter authentication

The voter first presents the RFID card to the RC522 module, and the card identity is looked up in the voter database. If the card is registered, the ESP32 camera captures the voter's face, which is matched against the photograph stored for that card. Finally the voter places a finger on the DY50 optical sensor and the fingerprint is compared with the enrolled template. The three checks run in sequence, and a failure at any stage stops the process, is logged as an authentication failure and is reported to the dashboard.

5.2 Duplicate-vote prevention and vote recording

Once identity is confirmed, the duplicate-vote check reads the voter's status in the cloud database. A voter already marked "Voted" is refused, even if the earlier vote was cast at another booth. Otherwise the voting interface is unlocked and the candidate push-buttons are enabled. When a button is pressed the vote is recorded and the voter's status is changed to "Voted" at once, which enforces the rule of one person, one vote in real time. Local processing can continue even during network problems.

5.3 Tamper detection and alerts

Tamper loop switches wired into the frame of the unit are watched continuously by the system tamper monitor. If the enclosure is opened or physically interfered with, the ESP32 activates the local alerts and sends a tamper alert through the remote IoT cloud, so that the election officer is informed immediately.

5.4 Dashboard, mobile application and administration

The admin dashboard presents voter verification results, votes cast, authentication failures, tamper alerts, live turnout and vote tallies to the election officer. An Android application with QR code scanning lets staff verify voter information quickly, and the booth hardware, the application and the cloud database are linked into one network. Officers can manage the voter database and review security logs remotely.

5.5 Comparison with the conventional polling process

Table -1 summarizes how the proposed system differs from present practice for the problems identified in Section 3.

Table -1: Conventional polling versus proposed system

Task	Conventional	Proposed
Identity check	Manual ID card inspection	RFID + face + fingerprint
Duplicate voting	Not tracked across booths	Cloud "Voted" status check
Booth tampering	No built-in detection	Tamper switches with alerts
Monitoring	No live view at headquarters	Real-time admin dashboard
Counting	Manual checks, physical transport	Live tallies on dashboard

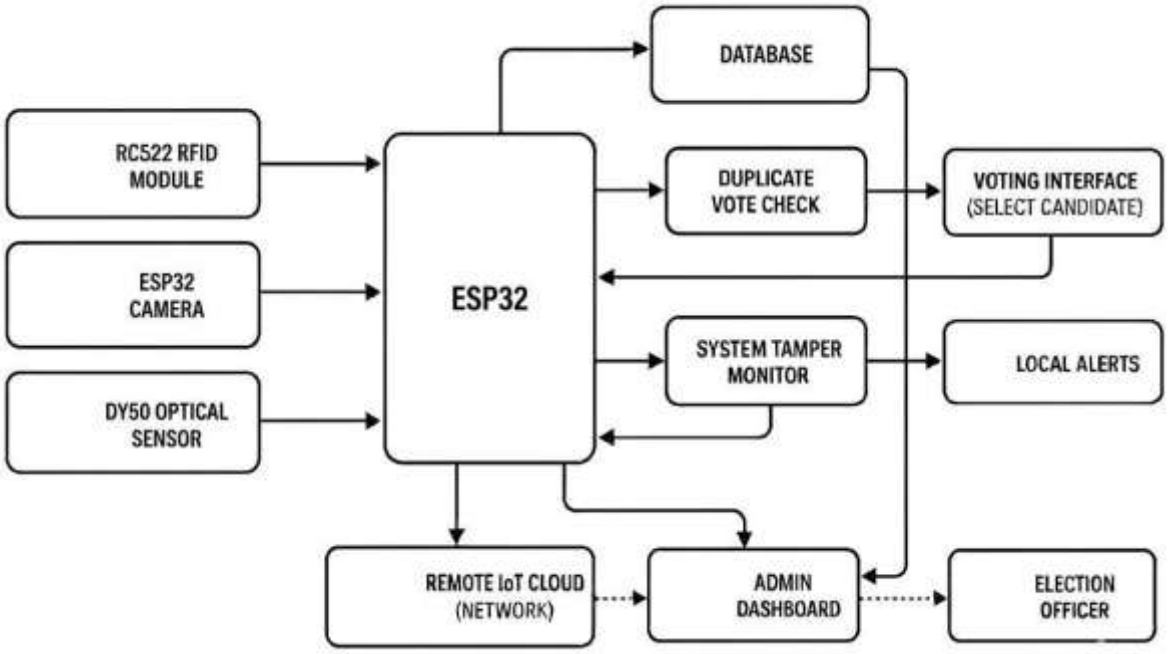


Fig -1: Block diagram of the AI-IoT based smart election authentication and integrity monitoring system

6. HARDWARE SETUP

The prototype uses the ESP32 controller, an ESP32 camera, an RC522 RFID reader with cards, a DY50 optical fingerprint sensor, tamper loop switches, candidate push-buttons, an OLED display, a buzzer and LED indicators, a power supply and an enclosure forming a mini polling booth. The work proceeds through requirements gathering, system design, hardware setup, Android application development, integration, testing with valid, duplicate and fake voters, deployment of the prototype with the live dashboard, and maintenance. The principal parts, with their approximate cost, are listed in Table -2.

Table -2: Major components and approximate cost

Sr. No.	Component	Qty.	Price (Rs.)
1	ESP32 DevKit	1	350-650
2	ESP32-CAM module	1	800
3	RC522 RFID reader	1	120
4	RFID cards/tags	10	25
5	DY50 optical fingerprint sensor	1	1200
6	0.96" OLED I2C display	1	200
7	Tamper loop / micro switches	4	30
8	Candidate push buttons	4	10
9	Buzzer	2	40
10	LEDs + 220/330 ohm resistors	1 set	50
11	Breadboard	2	150
12	Jumper wires	1 set	150
13	5V power supply	1	400
14	USB/FTDI programming cable	1 set	150
15	Project enclosure/acrylic booth model	1	700

The total outlay is estimated at about Rs. 7000, including spares and testing material, which is low enough for a student project and for small institutions to adopt.

7. CONCLUSIONS

SecureVoteGuard, an AI-IoT based smart election system built on an ESP32 controller, RFID, face recognition, fingerprint authentication and cloud storage, has been designed to address identity theft, double voting, booth tampering, the lack of live alerts and slow counting in conventional polling. The prototype is expected to deliver successful three-layer authentication, instant duplicate-vote elimination, immediate physical tamper alerts, live centralized data synchronization and a comprehensive real-time monitoring dashboard. Its low cost and modular structure make it suitable for demonstration and for further development towards larger deployments. The next steps are to build and test the prototype with valid, duplicate and fake voters, then to extend the design to multiple booths and use analytics to improve the service.

ACKNOWLEDGEMENT

The authors are grateful to the project guide, Prof. S. N. Wangikar, and to the Head of the Department, Prof. R. K. Gurav, Department of Electronics & Telecommunication Engineering, Dr. Daulatrao Aher College of Engineering, Karad, for their guidance and encouragement.

REFERENCES

[1] A. Manoj et al., "Next Generation Voting Approach: A Secured Biometric Voting System," IEEE, 2024.
[2] "Dual Authentication Voting System with Facial Recognition and Fingerprint Using CNN," IEEE, 2023.
[3] "Enhancing Voter Identity Verification Through Cloud Computing Enabled Biometric Authentication – Modern Voting," IEEE, 2024.
[4] "Fingerprint-Authenticated Voting System with Real-Time Data Sharing via Android Application," IEEE, 2025.
[5] S. Najam Syed, A. Z. Shaikh and S. Naqvi, "A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition."