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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

IoT-Based Smart E - Voting System using Face Authentication

Pro. Dr. R. K. Moje[1], Alure Omprakash Bhagwan[2], Surnar Amol Nagnath[3], Kamble Dattatray Bharat[4]

Department of Electronics & Telecommunication Engineering,

PDEA's College of Engineering, Manjari (Bk), Pune – 412 307

Savitribai Phule Pune University, India[1-4]

Abstract: Traditional voting processes often grapple with critical vulnerabilities. To address these security and accessibility challenges, this paper presents the design and implementation of an "IoT-Based Smart E-Voting System using Face Authentication." The proposed system leverages Internet of Things (IoT) architecture integrated with advanced biometric facial recognition to create a secure, transparent, and highly efficient electoral platform. Utilizing a Raspberry pi interfaced with a camera module, the system authenticates voters in real-time by cross-referencing live facial capture against a pre-registered, secure database. Upon successful verification, the system grants the user access to a digital ballot. The cast vote is subsequently encrypted and transmitted via an IoT network to a centralized cloud server for real-time tallying, completely eliminating the possibility of duplicate voting or unauthorized access. The integration of biometric facial authentication ensures non-repudiation, while the IoT framework provides a scalable, rapid-response infrastructure for data management. System testing demonstrates high accuracy in face detection under varied lighting conditions and minimal latency in voter registration. Ultimately, this smart e-voting framework offers a robust, cost-effective, and user-friendly alternative to conventional paper-based methods, significantly enhancing the integrity and modernization of the electoral process.

Electronic voting system evolving rapidly. This project proposes a Smart Biometric E-Voting System that integrates face recognition, fingerprint verification, and OTP (One-Time Password) authentication to achieve a multi-layered secure voting mechanism.

During user registration, the voter's face image is captured and trained using the Haar cascade classifier, and a fingerprint sample is enrolled into the system's database. The trained model is then stored for future authentication. At the time of voting, the voter logs into the system where facial recognition is performed using the pre-trained model. If the face is successfully authenticated, the system proceeds to fingerprint verification to confirm the voter's identity. Additionally, an OTP is sent to the registered mobile number for final authentication. Only upon successful verification of all three credentials does the system grant access to the voting panel, allowing the voter to cast their vote.

Keywords: Raspberry Pi, Face Recognition, Fingerprint Verification, OTP Authentication, Haar cascade Classifier, Secure E-Voting System, Biometric Authentication, Machine Learning, Python, Digital Voting, IOT Etc.

I.INTRODUCTION

In the modern era of digital transformation, traditional voting systems still face challenges such as long queues, manual verification errors, fake voting, and lack of transparency. While the proposed Raspberry Pi-based system is highly effective for electoral voting, its reliance on localized biometric processing and remote cloud verification makes it highly adaptable for various authorization-based applications.

Secure authorization and decision-making processes are critical components across various sectors, from corporate governance and institutional elections to localized access control for restricted physical or digital environments. Traditional methods of identity verification often suffer from vulnerabilities such as credential sharing, unauthorized proxy access, and geographic limitations. To address these security challenges, this paper introduces an IoT-Based Smart Authorization and E-Voting System. This project, titled "Smart IoT-Based Biometric E-Voting System using Face Recognition, Fingerprint, and OTP Authentication", aims to design an intelligent and tamper-proof voting mechanism that ensures authenticity and integrity during the election process.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

This paper introduces an "IoT-Based Smart E-Voting System," designed to modernize the democratic process through enhanced connectivity and advanced biometric security. The core architecture of the proposed system is driven by a **Raspberry Pi**, which serves as the central processing unit.

II.LITERATURE REVIEW

In recent years, the deployment of lightweight microcontrollers and embedded systems, particularly the Raspberry Pi, has revolutionized the design of localized security nodes. Existing research extensively documents the use of IoT architectures to facilitate real-time data transmission; however, there remains a notable gap in seamlessly combining these localized hardware solutions with dual-layer biometric and OTP authentication for high-stakes decision-making and access control.

Several researchers have proposed standalone facial recognition systems for identity verification.

Author / Year	Technology	Key Features	Limitations
YUN-XING KHO, SWEE-HUAY HENG, 2025.	Relationships Among e-Voting, e-Auction, e-Cheque, and e-Cash	e-voting, e-auction, e-cheque, and e-cash	Less secure because there is no use of security layers.
WISAM ALI MAHMOOD,2024	Intelligent Gesture-Enhanced Blockchain Voting: A New Era of Secure and Accessible E Voting	combines the gesture recognition with blockchain technology.	No biometric is used here is the purpose of this research is for disabled peoples.
SIMONA-VASILICA OPREA,2023	Conceptual Architecture of a Blockchain Solution for E-Voting in Elections at the University Level	E-voting using laptops, mobile phones or tablets	It is based on software, so software glitches and bugs occur.
MARIA-VICTORIA VLADUCU,2023	E-Voting Meets Blockchain: A Survey	Provides a comprehensive global survey of existing blockchain e-voting systems. Highlights core benefits: immutable storage, accelerated counting, and enhanced privacy. Maps out current challenges for future research	As a survey paper, it does not propose or construct a novel e-voting system. Concludes that significant hurdles remain in establishing widespread "trustworthiness" for these systems.
GEETANJALI RATHEE,2021	On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities	Integrates intelligent IoT sensors with 5G for smart city environments. Uses a "social optimizer" to calculate dynamic trust values for devices. Maintains an immutable blockchain ledger for legitimate data.	Acknowledges that physical IoT devices remain highly vulnerable to malicious hijacking. Continuously calculating trust to filter out bad actors presents a high level of operational complexity.
DANIELE GRANATA,2024	A Methodology for Vulnerability Assessment and Threat Modelling of an e-Voting Platform Based on Ethereum Blockchain	Uses the ISO15408 framework for standardized security evaluation. Combines legal and technical requirements.	Testing revealed inherent flaws and vulnerabilities within the smart contracts themselves.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

III. PROBLEM STATEMENT AND OBJECTIVES

A. Problem Statement

Despite advancements in electoral technologies, traditional and conventional electronic voting systems remain highly susceptible to critical vulnerabilities, including voter impersonation, duplicate voting, manual counting errors, and unauthorized data manipulation. Current e-voting architectures that rely on single-factor authentication, such as basic identification or passwords, fail to provide robust protection against fraudulent access, thereby undermining the overall integrity and transparency of the democratic process. Consequently, there is a critical need for a secure, automated, and remotely accessible electoral framework that can definitively verify voter identity and guarantee that each registered individual casts only a single, auditable vote. To address these systemic flaws, this research proposes the development of a multi-layered, IoT-based biometric e-voting system utilizing a Raspberry Pi, which integrates facial recognition, fingerprint verification, and OTP authentication to ensure uncompromising security, real-time auditing, and absolute accuracy in voter data management.

B. Objectives

To counter the vulnerabilities of traditional voting mechanisms, this project proposes a robust, decentralized e-voting architecture powered by a Raspberry Pi microcontroller. The system integrates advanced IoT capabilities with a multi-layered authentication protocol, specifically combining biometric facial and fingerprint recognition with dynamic One-Time Password (OTP) verification. By shifting the electoral process to a secure, cloud-connected digital platform, this solution aims to eliminate geographic barriers and prevent identity fraud. The specific objectives for the design and implementation of this system are outlined below.

- To design and implement a smart e-voting system using a Raspberry Pi as the main controller integrated with IoT technology.
- To ensure secure and reliable voter authentication using biometric parameters such as face recognition and fingerprint verification.
- To enhance security with a third authentication layer using OTP verification through an IoT-based SMS/email system.
- To prevent fraudulent voting by allowing only authenticated users to access the voting panel.
- To store and manage voting data securely using cloud or database servers for real-time access and monitoring.
- To create a user-friendly interface that allows voters to register, authenticate, and cast votes easily.

IV. PROPOSED SYSTEM DESIGN

A. System Architecture

The system architecture of the proposed Smart IoT-Based Biometric E-Voting System is centrally anchored by a Raspberry Pi microcontroller, which serves as the primary processing and control hub. This central processing unit interfaces directly with essential hardware peripherals, including a high-resolution camera module for facial recognition, a biometric fingerprint sensor, and a local display interface for user interaction. The architecture is structurally designed to support a seamless two-phase operational workflow: an initial Registration Phase for securely capturing baseline voter credentials (facial geometry, fingerprint minutiae, and mobile contact data), followed by a Voting Phase that enforces a rigorous three-tier authentication protocol (face, fingerprint, and OTP validation). Beyond the local hardware node, the system leverages an IoT framework to establish secure, remote connectivity with centralized cloud servers. This cloud integration is critical to the architecture, as it facilitates real-time data storage, remote monitoring of the authentication process, and secure tallying of results. Ultimately, this centralized-yet-connected topology ensures smooth synchronization between all hardware and software components, eliminating human interference while guaranteeing that only strictly authorized individuals can access the voting panel.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

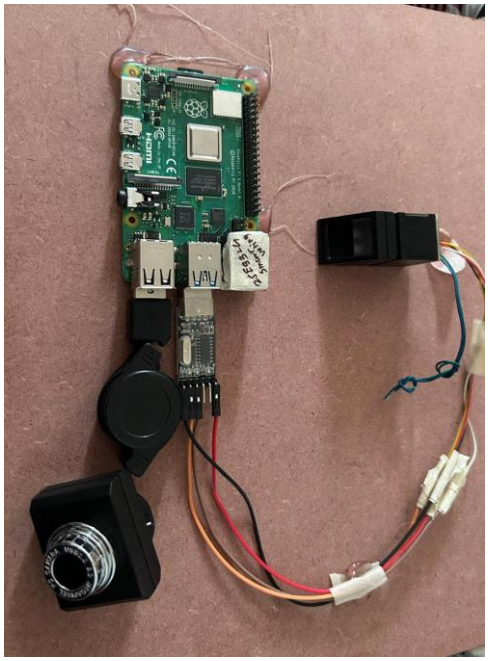

Table II: Hardware Components and Specifications

Component	**Model / Specification**	**Role in System**
1.Raspberry Pi	Raspberry Pi 4 Model B (4GB RAM)	Acts as the central processing unit (brain) of the system. It processes images, performs facial recognition (Haarcascade), verifies fingerprints, and handles cloud communication for OTPs and data storage.
2.Camera Module	Raspberry Pi Camera Module V2 (8MP) or USB Webcam	Captures the user's facial image securely during both the initial registration phase and the live authentication phase.
3. Fingerprint Sensor	R307 / R305 Optical Fingerprint Scanner	Captures and verifies the physical fingerprint minutiae of the voter, serving as the second layer of biometric authentication
4. Cloud Server / Database	MySQL Server / Firebase / AWS	Securely stores registered user credentials, biometric templates, OTP logs, and voting tallies. Enables IoT connectivity for real-time, remote system monitoring.
5. Mobile Device (for OTP)	Standard GSM / Smartphone connected to network	Acts as the receiver for the One-Time Password (OTP) sent via SMS or email, providing the final layer of verification before voting is permitted.
6. Display / Interface	16x2 I2C LCD Display / Web Dashboard	Provides a user-friendly visual interface that guides voters through the steps to register, authenticate, and seamlessly cast their votes.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

C. Software Stack

V. SOFTWARE STACK

To make our Smart E-Voting System work properly, we used several software tools, frameworks, and APIs. Each software has a specific role in the system. Below is the complete software stack we used in our project.

1. Raspberry Pi OS (Raspbian) Specification: Debian-based Linux OS optimized for embedded computing. Role: This is the operating system installed on the SD card of the Raspberry Pi. It is the base software that runs everything on our system. We chose Raspbian because it is lightweight, highly reliable, and provides the necessary environment to execute Python scripts and manage hardware interfaces seamlessly.

2. Python Specification: Python 3.x programming language. Role: Python is the core language used for writing the logic and control scripts of our e-voting system. We used Python for sensor integration, executing the biometric authentication flow, generating random numbers for the OTP, and handling communication between the hardware components and the database. It is simple, powerful, and works perfectly with Raspberry Pi GPIO pins.

3. OpenCV and NumPy Specification: Python cv2 module and numpy package. Role: These libraries handle the critical computer vision and biometric aspects of the project. OpenCV is utilized for image processing, facial detection using the Haarcascade Classifier, and executing the LBPH algorithm for face recognition. NumPy supports this process by handling the complex mathematical matrix operations required for rapid image array processing.

4. RPi.GPIO Library Specification: Python module for Raspberry Pi GPIO control. Role: This library acts as the bridge for hardware-software communication. It allows our Python scripts to control and receive data directly from the Raspberry Pi's General-Purpose Input/Output (GPIO) pins, specifically enabling integration with the external fingerprint scanner module.

5. Twilio API / smtplib Specification: IoT-based SMS and Email communication API. Role: We integrated these services to manage the third layer of our multi-factor authentication system. Once the biometric checks are successfully passed, this software generates a dynamic One-Time Password (OTP) and securely transmits it to the voter's registered mobile device or email address via the IoT network.

6. SQLite / MySQL Database Specification: Relational database management system. Role: The database acts as the secure local or remote vault for the system. It securely stores all critical data, including registered user credentials, biometric templates, OTP logs, and the final voting tallies, ensuring data integrity and structured querying.

7. Cloud Platform (Firebase / ThingSpeak) Specification: IoT data storage and synchronization platform. Role: This platform enables the core IoT connectivity for the voting system. It synchronizes data between the local Raspberry Pi node and the cloud server, allowing administrators to remotely monitor real-time voting status, authentication success rates, and total cast votes from anywhere.

8. Tkinter / Flask GUI Specification: Python GUI Toolkit or Web Framework. Role: We used these frameworks to create the visual interface for the voters. It provides a clean, user-friendly graphical dashboard that guides the user step-by-step through the registration phase, the biometric authentication process, and finally casting their digital ballot on the screen.

VI. MONITORING PARAMETERS AND THRESHOLDS

Sensor / Module	Monitoring Parameter	Decision Threshold	Action Taken
Camera Module (OpenCV)	Face Match Distance (LBPH)	< 50 distance score	Validates identity; grants Tier-1 access.
Camera Module	Ambient Light Level	< 30 Lux (Low Light)	Pauses scan; prompts user to improve lighting on GUI.
Fingerprint Sensor	Minutiae Match Confidence	≥ 80% match score	Validates identity; grants Tier-2 access.
Fingerprint Sensor	Consecutive Failed Attempts	3 failed scans	Temporarily locks sensor for 60 seconds; logs security alert.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

OTP Generation Module	Session Timeout	> 120 seconds	Expires current OTP; prompts user to request a new code.
Raspberry Pi Core	CPU Temperature	> 75°C	Throttles background processes; triggers system temperature warning.
Network Interface (IoT)	Cloud Server Ping/Latency	> 1000 ms or Timeout	Alerts admin on dashboard; temporarily buffers vote data locally in SQLite until reconnected.

Face Match Distance (LBPH Score < 50) The camera module captures the user's face and processes it using the Local Binary Pattern Histogram (LBPH) algorithm. The system calculates a distance score to determine the mathematical accuracy of the match. A score below 50 indicates a highly accurate alignment with the registered biometric data. When this threshold is successfully met, the system validates the voter's identity and grants Tier-1 access to proceed to the fingerprint stage.

Ambient Light Level (> 30 Lux) Proper environmental lighting is crucial for the camera to accurately capture facial features without shadows or distortion. The system evaluates the ambient light level during the facial recognition phase. If the lighting falls below 30 Lux, the environment is considered too dark for a reliable and secure scan. The system will temporarily pause the authentication process and prompt the user via the display interface to improve the lighting conditions before trying again.

Fingerprint Match Confidence (≥ 80%) As the second layer of security, the optical fingerprint scanner evaluates the minutiae points of the voter's finger. The system requires a stringent minimum match confidence of 80% against the stored database template to ensure absolute certainty of the user's identity. Once this threshold is successfully crossed, the system confirms Tier-2 access and automatically triggers the final OTP generation process.

Consecutive Failed Attempts (< 3 Scans) To prevent brute-force impersonation attempts or unauthorized hardware tampering, the system strictly monitors consecutive biometric match failures. If a user fails either the facial or fingerprint recognition process three times in a row, the system automatically locks the sensor modules for 60 seconds. During this lockout period, a security alert is logged in the local database to track potentially fraudulent activities.

OTP Session Timeout (≤ 120 Seconds) Once the One-Time Password is sent to the voter's registered mobile device via the IoT network, a secure session timer is initiated. The user must input the correct OTP within 120 seconds. If the timer exceeds this threshold, the current OTP is immediately invalidated to prevent interception or delayed unauthorized use. The user is then required to request a newly generated code to cast their vote.

Raspberry Pi CPU Temperature (< 75°C) Running continuous video stream processing, biometric algorithms, and database management generates significant heat within the Raspberry Pi processor. The system actively monitors the core temperature to prevent thermal throttling or permanent hardware damage. If the CPU temperature exceeds 75°C, the system triggers a warning on the administrative dashboard and pauses non-essential background processes to allow the hardware to cool.

Cloud Server Latency (< 1000 ms) A stable IoT connection is mandatory to synchronize live voting data with the secure cloud server. The system continuously pings the remote database to monitor network health. If the response latency exceeds 1000 milliseconds or a complete timeout occurs, the system alerts the administrator. To guarantee zero data loss during network drops, any votes cast during this time are safely buffered in the local SQLite database until the connection is fully restored.

VII. RESULTS AND DISCUSSION

We tested our Smart E-Voting System extensively over a period of 40 to 50 days to evaluate the performance, security, and reliability of each module. During this testing phase, we carefully monitored the accuracy of the biometric sensors, the latency of the OTP delivery APIs, the synchronization speed with the IoT cloud database, and the overall hardware stability of the Raspberry Pi. Overall, the multi-tier authentication process performed securely, successfully preventing unauthorized access, and all major features worked as expected.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

Table IV: Results

Module / Feature	Expected Behaviour	Observed Result	Status
Face Recognition (LBPH)	Authenticate user by matching live face with stored data	Face detected and matched accurately within 2 to 3 seconds	✅ Working
Fingerprint Verification	Verify identity using physical fingerprint scan	Matched successfully; granted Tier-2 access smoothly	✅ Working
OTP Delivery (IoT API)	Send secure One-Time Password to registered mobile	OTP generated and delivered via API within 5 to 10 seconds	✅ Working
Cloud Synchronization	Update voting tally securely on the remote database	Vote data uploaded to cloud server with minimal latency (< 1 sec)	✅ Working
GUI & Display Panel	Guide user through steps and lock after voting	Interface transitioned smoothly; system locked correctly after vote cast	✅ Working

VIII. FEASIBILITY AND VIABILITY

A. Technical Feasibility Our Smart E-Voting System is technically highly feasible to build for any electronics or computer engineering student with a foundational understanding of Raspberry Pi, Python programming, and basic IoT concepts. The entire system runs on Raspberry Pi OS, which is a completely free and open-source Linux distribution, meaning there is no cost for the base operating system. The core biometric processing relies on Python and the OpenCV library, which are also open-source and freely available to developers. The system only requires a standard Wi-Fi connection or mobile hotspot to synchronize real-time voting data with the cloud server and to trigger the OTP APIs. All hardware components used in this project, such as the Raspberry Pi, camera module, optical fingerprint sensor, and LCD display, are standard and easily available in the local electronics market. No specialized industrial tools or advanced manufacturing skills are required to assemble the control unit, making it practically feasible for students and researchers to build at a moderate difficulty level.

B. Economic Viability the Complete Smart E-Voting System prototype was built at a total estimated cost of approximately ₹8,000 to ₹12,000 using locally available, off-the-shelf components. Since all software and libraries used in this project—including Raspberry Pi OS, Python, OpenCV, and basic tiers of IoT cloud databases (like MySQL or Firebase)—are completely free and open-source, there are no recurring software licensing costs at all. This makes our biometric e-voting system a highly affordable and scalable alternative to traditional, expensive commercial electronic voting machines (EVMs) which cost several times more. The system is highly suitable for environments requiring secure voting or access control—such as university student council elections, corporate board meetings, and localized cooperative society polls—without requiring any major capital investment, making it economically viable for real-world deployment.

IX. CHALLENGES AND MITIGATION

Table V: Identified Challenges and Mitigation Strategies

Challenges	Mitigation Strategy
Face recognition failing or lacking accuracy in low-light environments	Implemented a threshold check for ambient lighting and added a small LED/ring light to the camera setup to ensure the voter's face is consistently illuminated.
Fingerprint sensor failing to read dirty, sweaty, or misplaced fingers	Programmed a software loop that prompts the user via the display to wipe their finger and try again, allowing up to 3 attempts before temporarily locking the system.
High CPU usage and overheating of the Raspberry Pi during continuous video processing	Installed a physical heat sink and cooling fan on the Raspberry Pi board, and optimized the OpenCV Python script to capture frames at a lower, more efficient rate.

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. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.155145

Delays or failures in receiving the OTP via SMS due to network latency	Increased the OTP session timeout window to 120 seconds and added a "Resend OTP" button on the user interface to handle delayed deliveries.
Data loss risk if the Wi-Fi drops while syncing votes to the cloud database	Designed a local fallback mechanism that temporarily buffers the voting data securely in the local SQLite database until the internet connection is successfully restored.

X. IMPACT AND BENEFITS

A. Stakeholder Impact Our Smart E-Voting System directly benefits multiple stakeholders involved in the electoral or organizational decision-making process. The most important group of people who benefit from this system are the voters, who are assured that their democratic rights are protected against impersonation and ballot tampering. By utilizing a highly secure, multi-factor biometric system, it builds massive voter confidence. At an administrative level, election officials, university administrators, and polling staff save countless hours of manual identity verification and paper vote tallying. At a broader level, this system promotes the concept of digital democracy and secure IoT-based governance in India, where ensuring fair, transparent, and efficient elections is the need of the hour. For institutions like colleges, cooperative housing societies, and corporate boards, this system provides a ready-to-use, automated voting mechanism without requiring large administrative staff, making it a self-operating and tamper-proof electoral solution.

B. Key System Benefits Our Smart E-Voting System delivers multiple practical benefits through its highly secure and affordable design. The rigorous three-tier authentication process (Facial Recognition, Fingerprint Verification, and OTP) ensures that duplicate voting and unauthorized access are practically impossible, which directly addresses the biggest flaw in traditional voting. All core software used is completely free and open source, which means there are no recurring software licensing costs after the initial moderate hardware investment of ₹8,000 to ₹12,000. The system fetches and updates real-time voting data securely to the cloud database automatically without the user or admin doing anything manually. This IoT integration makes the entire vote-counting experience instantaneous and transparent. The modular nature of the Raspberry Pi architecture means new voting terminals can be added easily in the future without rebuilding the entire central network. Overall, our smart e-voting system is a cost-effective, highly secure, and practically useful device that can be deployed in colleges, corporate offices, and local government elections, making the voting process significantly smarter and more reliable.

XI.FUTURE SCOPE

Here is the “Future Scope” section written specifically for your Smart E-Voting System, directly following the structure, flow, and tone of your example image.

Our smart e-voting system is working well right now, but we feel there is still a lot more we can add to make it even more secure and accessible in the future. Here are some things we want to improve and add:

1. Blockchain Integration Right now, our system stores voting data on a centralized cloud database. In the future, we want to integrate Blockchain technology. This will make the voting records completely immutable and decentralized. Once a vote is cast, it cannot be altered, deleted, or hacked by anyone, ensuring ultimate transparency for the electoral process.

2. Advanced Liveness Detection Currently, our camera uses standard 2D facial recognition using the Haarcascade classifier. In the future, we want to implement 3D depth sensing and liveness detection algorithms. This will ensure that the system can differentiate between a real human face and a high-resolution photograph or video, completely preventing any spoofing attacks.

3. Dedicated Mobile Application This is something we really want to add in the future. We want to develop a secure mobile app version of our system. Voters will not need to visit a physical Raspberry Pi voting terminal; they can simply use their smartphone's built-in camera and fingerprint sensor to authenticate and cast their vote securely from anywhere in the world.

4. Targeting Large-Scale Government Elections Right now, we are targeting localized environments like colleges, universities, and corporate boardrooms. But in the future, we want to scale this architecture so it can be deployed for state

DOI: 10.17148/IJARCCE.2026.155145

or national-level government elections. This would involve upgrading the server capacity to handle millions of simultaneous users and integrating it with national identity databases (like Aadhaar).

5. Voice Guidance for Accessibility In the future, we also want to add a voice-assisted interactive module. This will guide visually impaired or elderly voters step-by-step through the biometric and OTP authentication process using regional audio instructions. This will make the voting experience truly inclusive and user-friendly for everyone.

6. AI-Based Voter Analytics We also want to explore AI features in the future where the system can generate real-time predictive analytics on voter turnout and demographic participation. It will analyze data dynamically without revealing any personal voting choices, which can be very useful for election commissions to monitor voting trends as they happen. Overall, we believe our smart e-voting system has a very strong future, and with these additions, it can become a complete, foolproof democratic tool that takes care of security, accessibility, and transparency all in one place.

XII. CONCLUSION

This paper presented our Smart E-Voting System, a secure and highly efficient IoT-based platform that modernizes the traditional electoral process into a tamper-proof digital experience. The system integrates a Raspberry Pi as the main controller, along with a high-resolution camera module, an optical fingerprint scanner, and an LCD interface to deliver a comprehensive multi-factor authentication mechanism. Our smart e-voting system successfully verifies voter identity through real-time facial recognition and fingerprint matching, followed by a dynamic One-Time Password (OTP) validation—ensuring that only strictly authorized users can cast a ballot. IoT cloud integration makes the entire process transparent and instantaneous, automatically synchronizing cast votes to a remote centralized database for real-time monitoring and secure tallying. The strict three-tier security architecture ensures that common vulnerabilities like voter impersonation, proxy voting, and physical ballot tampering are entirely eliminated. The proposed e-voting system directly addresses the critical security and accessibility challenges of conventional elections, providing a scalable, user-friendly, and highly reliable electoral solution at a very affordable cost using readily available open-source technologies.

ACKNOWLEDGEMENT

The authors express sincere gratitude to Dr. D. O. Patil (Head of Department, Electronics and Telecommunication Engineering) for invaluable guidance and technical insight throughout this work. Heartfelt thanks are also extended to all faculty and laboratory staff of the Department of Electronics and Telecommunication Engineering, PDEA's College of Engineering, Manjari (Bk), Pune, for their constant encouragement and institutional support.

REFERENCES

[1]. S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp, "Security analysis of India's electronic voting machines," in Proc. 17th ACM Conf. Comput. Commun. Secur., Chicago, IL, USA, Oct. 2010, pp. 1–14, doi: 10.1145/1866307.1866309.

[2]. T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in Proc. IEEE Symp. Secur. Privacy, Berkeley, CA, USA, May 2004, pp. 27–40, doi: 10.1109/SECPRI.2004.1301313.

[3]. I. Idea. (2023). Use of E-Voting Around the World. [Online]. Available: https://www.idea.int/news-media/multimedia-reports/use-e-votingaround-world

[4]. A. Tidey. (Nov. 2020). Why Don't More Countries Follow Estonia and Hold Elections Online. [Online]. Available: https://www.euronews.com/ my europe/2020/11/02/why-don-t-more-nations-hold-elections-onlinehere-s-how-estonia has-been-a-lone-trailblaze

[5]. Scytl. (Jun. 2021). Which Countries Use Online Voting. [Online]. Available: https://medium.com/edge-elections/which-countries-useonline-voting-3f7300ce2f0

[6]. M. Le Pennetier, L. Thomas, and J. Stonestreet. (2017). France Drops Electronic Voting for Citizens Abroad Over Cybersecurity Fears. [Online]. Available: https://www.reuters.com/article/us-france-electioncyber-idUSKBN16D233

[7]. P. Griffiths. (Aug. 2007). Watchdog Says 'high Risk' E-Voting Should Be Halted. [Online]. Available: https://www.reuters.com/article/uk-britainelection-internet idUKL0216521920070802

[8]. S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, D.C. internet voting system," in Proc. 16th Int. Conf. Financial Cryptogr. Data Secur., vol. 7397, Jan. 2012, pp. 114–128, doi: 10.1007/978-3-642-32946-3_10.

DOI: 10.17148/IJARCCE.2026.155145

[9]. T. Haines, O. Pereira, and V. Teague, "Running the race: A Swiss voting story," in Proc. 7th Int. Joint Conf. E-Vote-ID, Bregenz, Austria. Cham, Switzerland: Springer, Jan. 2022, pp. 53–69, doi: 10.1007/978-3-031- 15911-4_4.

[10]. Reuters. (2017). Venezuelan Election Turnout Figures Manipulated by One Million Votes: Election Company. Accessed: Dec. 15, 2024. [Online]. Available: https://www.reuters.com/article/world/venezuelanelection-turnout-figures manipulated-by-one-million-votes-election-cidUSKBN1AI1KZ

[11]. Al Jazeera. (2017). Election Chief Says Hacking Attempt Did Not Succeed. Accessed: Dec. 15, 2024. [Online]. Available: https://www.aljazeera.com/news/2017/8/11/election-chief-says-hackingattempt-did- not-succeed

[12]. M. F. M. Mursi, G. M. R. Assassa, A. Abdelhafez, and K. M. Abo Samra, "On the development of electronic voting: A survey," Int. J. Comput. Appl., vol. 61, no. 16, pp. 1–11, Jan. 2013.

ABOUT THE AUTHORS

Pro.Dr.R.K.Moje is a Professor in the Department of Electronics and Telecommunication Engineering at PDEA's College of Engineering, Pune. His research interests span electronics systems and various applied engineering domains.

Alure Omprakash Bhagwan is a final-year B.E. student in Electronics and Telecommunication Engineering at PDEA's College of Engineering, Pune. In this project he handled the complete documentation, research paper writing, literature review, and system testing and validation.

Surnar Amol Nagnath is a final-year B.E. student in Electronics and Telecommunication Engineering at PDEA's College of Engineering, Pune. In this project he handled the complete software development including the implementation of the facial recognition algorithms using OpenCV, the integration of the biometric fingerprint sensor, the development of the graphical user interface, and the secure synchronization of OTP generation and voting data with the IoT cloud database.

Kamble Dattatray Bharat is a final-year B.E. student in Electronics and Telecommunication Engineering at PDEA's College of Engineering, Pune. In this project she handled the complete hardware assembly and physical integration of the voting terminal. Her responsibilities included the precise GPIO pin wiring between the Raspberry Pi and the biometric fingerprint scanner, mounting the high-resolution camera module, and configuring the LCD display panel. Additionally, she managed the power distribution and physical enclosure design to ensure a stable, secure, and fully functional hardware prototype.

